Demostraciones varias de la infinidad de números primos

Alexander Guadalupe Vázquez Marín

Abril 2024

1. Introducción

La teoría de números, la reina de las matemáticas según Gauss, posee una fascinante capacidad para unir diversos campos matemáticos. Un claro ejemplo de este entrelazamiento se manifiesta en la demostración de la infinitud de los números primos, un resultado fundamental y sencillo de enunciar, pero que es de gran importancia pues responde una interrogante inherente a un objeto tan importante de la matemática, los números primos. Si bien Euclides nos legó una demostración elemental y elegante basada en el método de contradicción, a lo largo del tiempo han surgido demostraciones alternativas que se apoyan en herramientas analíticas, topológicas, algebraicas, etc. Todas ellas igual de fascinantes y que hacen énfasis en el como es posible usar las herramientas de una rama de las matemáticas en otra rama aparentemente desconectas. Todo esto hace que nos cuestionemos si en verdad es correcto usar el termino matemáticas y no en su forma singular matemática.

2. Demostraciones de la infinidad de primos

Antes de comenzar con las demostraciones es necesario definir lo que es un número primo:

Definición 1. *Se dice que un número natural n es primo si $n > 1$ y los únicos divisores de n son n y 1. Aquí una lista de los primeros números primos:* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37...$

Nota: Resulta curioso para muchas personas el porqué 1 no es considerado un número primo. Cierto es que 1 cumple con la condición de ser divisible por 1 y por sí mismo, entonces, ¿por qué se exige la extraña condición de que $n > 1$? Muchos matemáticos atribuyen esto al hecho de que, al definir a los números primos de esta manera, aseguramos que se cumpla un teorema importante: el Teorema Fundamental de la Aritmética (sabemos que un teorema es importante cuando tiene un nombre pomposo). Este teorema establece que todo número mayor a 1 puede expresarse de manera única como producto de números primos.

Si 1 fuese considerado un primo, entonces este teorema no se cumpliría, ya que un número como 6 no tendría una representación única en términos de números primos: $6 = 2 * 3 = 1 * 2 * 3 = 1 * 1 * 1 * 1 * 2 * 3$.

2.1. Demostración de Euclides

Primero demostremos el siguiente lema:

Lema 1. *Todo natural $n > 1$ cumple ser un número primo o un producto de números primos.*

Demostración. Para demostrar esto haremos inducción fuerte sobre n. Primero notemos que el teorema es cierto para $n = 2$, pues sus únicos divisores son 1 y 2. Ahora asumimos que $n > 2$ y que el teorema se cumple para todo natural mayor que 2 y menor que n. Ahora demostremos que el teorema se cumple para n, para ello consideremos dos casos.

1. Si n es primo es claro que se cumple el teorema.
2. Si n no es primo entonces se puede expresar como: $n = ab$ donde $1 < a, b < n$, usando la hipótesis de inducción, a, b son primos o producto de primos, por lo que $n = ab$ es un producto de números primos y el teorema se verifica.

□

Teorema 1. *Hay una infinidad de números primos*

La siguiente demostración hecha por contradicción es en mi opinión una de las más bellas en la matemática por la simplicidad de los argumentos y por la importancia del resultado.

Demostración. Asumamos que existe una cantidad finita de números primos, digamos $p_1, p_2, ..., p_n$. Sea $N = 1 + p_1 p_2 ... p_n$. Ahora como $N > 1$ por el lema anterior, N debe ser un número primo o un producto de números primos. Como construimos N para no ser un número primo pues es mayor a todos los p_i, entonces N debe ser un producto de primos es decir N debe ser divisible por un p_k entonces $N = c * p_k = p_1 p_2 ... p_n + 1$ despejando $1 = p_k(c + p_1 p_2 ... p_n)$ lo cual no puede suceder pues el único número que divide al 1 es el 1 Esto nos lleva a una contradicción por lo que hay una cantidad infinita de números primos □

resivir

2.2. Demostración de Clarkson

La siguiente demostración usa herramientas el análisis matemático que demuestra un resultado igualmente interesante del cual la infinidad de números primos se puede obtener como corolario.

Teorema 2. *La serie $\sum_{n=1}^{\infty} p_n$ diverge.*

Demostración. Procedemos por contradicción y demostramos que la serie converge. Si la serie convergiera entonces existe un entero k tal que

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}$$

(Para convencerse de esto el lector puede intentar demostrar que dada una serie convergente de terminos positivos entonces dado $\epsilon > 0$, existe $k \in \mathbb{N}$, tal que $\sum_{k+1}^{\infty} < \epsilon$)

Ahora definamos $Q = p_1...p_k$ y consideremos los números $1 + nQ$ para cada $n \in \mathbb{N}$ Ninguno de estos números es divisible por alguno de los primos $p_1, p_2, ..., p_k$ pues si este fuera el caso $1 + nQ = c * p_i$ para algún i entre 1 y k, luego $1 = p_i(c - n(p_1p_2...p_{i-1}p_{i+1}...p_k))$. De esto tenemos que todos los factores de $1+nQ$ ocurren en los primos $p_{k+1}, p_{k+2}, ...$ Entonces para cada $r \geq 1$ tenemos que:

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} (\sum_{m=k+1}^{\infty} \frac{1}{p_m})^t$$

Está desigualdad se cumple porque la suma en la derecha incluye todos los términos de la suma en la izquierda. Por otra parte como $(\sum_{m=k+1}^{\infty} \frac{1}{p_m})^t \leq (\frac{1}{2})^t$ para cualquier t, es decir los términos de la serie están acotados por los términos de la serie geométrica.

$$\sum_{t=1}^{\infty} (\frac{1}{2})^t$$

Y como la serie geométrica es convergente y acota a la que propusimos, entonces la serie $\sum_{n=1}^{\infty} \frac{1}{1+nQ}$ cumple que la sucesión de sumas parciales es monótona y acotada por lo que es convergente, sin embargo esto es una contradicción. Porque utilizando el teorema de comparación esa serie diverge. Así concluimos que $\sum_{n=1}^{\infty} p_n$ diverge.

□

Finalmente el hecho de que existe una infinita cantidad de números primos es un corolario del teorema anterior, pues la suma solo diverge si tiene una cantidad infinita de términos.

Coroloario 1. *Hay una cantidad infinita de números primos*

2.3. Demostración de Furstenberg

La siguiente demostración publicada por el matemático Hillel Furstenberg, cuando aún era estudiante de licenciatua en 1955, usa herramientas puramente topologicas

Teorema 3. *Existe una infinidad de números primos.*

Demostración. Definamos una topología sobre los enteros $\mathbb{Z}$ conocida como topología entera uniformemente espaciada, que se define de la siguiente manera. Sea $U \subset \mathbb{Z}$, se dice que U es abierto si y solo si se puede expresar como la unión de conjuntos $S(a,b)\, a, b \in \mathbb{Z}$ con $a \neq 0$. $S(a,b) = \{an + b | n \in \mathbb{Z}\} = a\mathbb{Z} + b$

De manera equivalente, U se dice que es abierto si y solo si para cada $x \in U$ existe un entero $a \neq 0$ tal que $S(a,x) \subset U$. Ahora verifiquemos que hemos definido una topología de $\mathbb{Z}$.

1. Es claro que $\emptyset$ es abierto pues se puede expresar como unión vacia, mientras que $\mathbb{Z}$ es la secuencia $S(1,0)$ así que también es abierto.

2. Dada una colección de abiertos U_i al considerar su unión U, dado un $x \in U$, por estar en la unión $x \in U_k$ para algún k, luego, $S(a,x) \subset U_k \subset U$. Luego U es abierto, por lo que la unión arbitraria de conjuntos abiertos es abierto.

3. La intersección de dos (y, por lo tanto, de una cantidad finita) conjuntos abiertos es un conjunto abierto. Dados U_1 y U_2 abiertos, sea $x \in U_1 \cap U_2$. Por ser abiertos, tenemos que $S(a_1,x) \subset U_1$ y $S(a_2,x) \subset U_2$, donde $S(a,x)$ denota la esfera de radio a centrada en x. Considerando b como el mínimo común múltiplo de a_1 y a_2, entonces $S(b,x) \subset U_1 \cap U_2$. Por lo tanto, $U_1 \cap U_2$ es un conjunto abierto.

Con esto tenemos que en efecto hemos definido una topología. Ahora está topología cumple con dos propiedades importantes:

1. Ahora como todo conjunto abierto distinto del vacío cubre a un $S(a,b)$ y este conjunto es infinito, tenemos que todo abierto debe ser infinito, que es equivalente a que ningún conjunto finito puede ser abierto, lo que implica que el complemento de un conjunto finito, no vacío no puede ser un conjunto cerrado.

2. el conjunto de los $S(a,b)$ con $a, b \in \mathbb{Z}, a \neq 0$ forman una base de la topología, y además son abiertos por definición y son cerrados porque podemos escribir a $S(a,b)$ como el complemento de un abierto de la siguiente manera
$$S(a,b) = \mathbb{Z} \bigcup_{j=1}^{a-1} S(a, b+j)$$

Ahora notemos que los únicos enteros que no son múltiplos de primos son el -1 y $+1$, luego:
$$\mathbb{Z}\{+1,-1\} = \bigcup_{p \text{ primo}} S(p,0)$$

Ahora por la primera propiedad el conjunto de la izquierda no puede ser cerrado, mientras que por otra parte por la segunda propiedad cada uno de los $S(p,0)$ es un conjunto cerrado. Por lo que si tuviéramos una cantidad finita de números primos entonces el conjunto de la derecha sería cerrado pues sería la unión finita de conjuntos cerrados, pero esto sería una contradicción, por lo que existe una cantidad infinita de números primos.

□

2.4. Demostración con sucesion de coprimos

Teorema 4. *Todos los términos de la sucesión* $a_n = 2^{2^n} + 1$ *son coprimos en pares.*

Demostración. Usando inducción es simple demostrar que:

$$2^{2^n} - 1 = (2^{2^1} - 1) \prod_{m=1}^{n-1} (2^{2^m} + 1)$$

De esta manera tenemos que, para cada $m < n$, se cumple que $(2^{2^m} + 1, 2^{2^n} + 1) | (2^{2^n} - 1, 2^{2^m} + 1)$ Esto demuestra que todos los términos de las sucesión son coprimos en pares.Y como al menos un número primo debe dividir a cada término de la sucesión y por ser coprimos todos estos primos deben ser distintos y como tenemos una infinidad de términos en la sucesión entonces debe existir una infinita cantidad de números primos. □

2.5. Demostración por conteo de la infinidad de primos

Antes de iniciar primero definamos la siguiente función.

Definición 2. *En teoría de números la función contador de números primos* $\pi(n)$ *cuenta la cantidad de números primos menor o igual a un cierto* n. $\pi(n) = card(\{p \in \mathbb{P} | p \leq n\})$

Ahora iniciemos con la demostración

Teorema 5. *La función contador de números primos está acotada inferiormente por una función que tiende al infinito cuando* n *tiende al infinito.*

Demostración. La factorización de cualquier entero menor o igual a n tiene la forma $\prod p_k^{e_k}$ donde:

$$\sum_{k=1}^{\pi(n)} e_k log p_k \leq log n$$

entonces se sigue que $e_k \leq log_2 n$ para todo k, luego $n \leq (log_2 n + 1)^{\pi(n)}$ Esto nos da la siguiente desigualdad la cual es una versión extremadamente débil del Teorema de los números primos.

$$\pi(n) \leq \frac{log n}{log(log_2 n + 1)}$$

Con esto podemos concluir que existe una infinidad de números primos.

□

3. Otros teoremas importantes de los números primos

3.1. Distancias infinitamente grandes entre primos

3.2. Conjetura de los gemelos

3.3. Conjetura de Goldbach

3.4. La distribución de los números primos

4. Cálculo de números primos

5. Primos generalizados, anillos y dominios enteros

6. Curiosidades

El número 57 es conocido como el "primo de Grothendieck", aunque en realidad no es un número primo, ya que se puede factorizar como $57 = 319$, se le considera como "primo.ª modo de broma debido a una anécdota en la que Alexander Grothendieck, uno de los más importantes de la era moderna, utilizó el número 57 como ejemplo de un número primo.

Referencias

[1] Tom M. Apostol, *Analytic Number Theory*, Springer, 1976.

[2] On the Infinitude of Primes on JSTOR. (s. f.). JSTOR. `https://www.jstor.org/stable/2307043?origin=crossref`