Una demostración de la infinitud de los números primos usando funciones

Miguel Angel Mejía Galindo

21 de octubre de 2025

Nuestro principal resultado es el siguiente:

Teorema 1. Si $\mathrm{Cop}_*(X)$ es un conjunto finito de números entonces X es un conjunto infinito de números.

El resultado anterior lo obtendremos demostrando su contrapuesta, la cual nos dice que todo conjunto finito de números posee una cantidad infinita de números coprimos en común. Lo cual es una generalización de un argumento que se da en la demostración clásica de la infinitud de los números primos, en especifico es el argumento para generar un nuevo número a partir de una lista finita de números primos.

Comenzamos definiendo la relación binaria $\mathrm{Cop} \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$, donde $n\ \mathrm{Cop}\ m$ si n es coprimo con m, o equivalentemente, si $\mathrm{MCD}(n,m) = 1$. Ahora, a partir de esta relación definimos la función $\mathrm{Cop}_* \colon \wp(\mathbb{Z}^+) \to \wp(\mathbb{Z}^+)$ con la regla de correspondencia

$$X \mapsto \{m \in \mathbb{Z}^+ \mid \forall n \in X, n\mathrm{Cop}m\}.$$

Una consecuencia inmediata de la definición es la siguiente igualdad:

$$\mathrm{Cop}_*(X) = \bigcap_{x \in X} \mathrm{Cop}_*(X).$$

Así, si $\mathbb{P}$ es el conjunto de números primos, entonces

$$\mathrm{Cop}_*(\mathbb{P}) = \bigcap_{p \in \mathbb{P}} \mathrm{Cop}_*(\{p\}).$$

Por lo que, para saber quien es $\mathrm{Cop}_*(\mathbb{P})$, solo debemos preguntarnos quien es $\mathrm{Cop}_*(\{p\})$.

Proposición 1. Si p es un número primo, entonces $\mathrm{Cop}_*(\{p\}) = \mathbb{Z}^+ \setminus p\mathbb{Z}^+$.[1]

Demo: Si $y \in \mathrm{Cop}_*(\{p\})$, entonces por definición $\mathrm{MCD}(p,y) = 1$. Luego, si por contradicción suponemos que existe $k \in \mathbb{Z}^+$ tal que $kp = y$, entonces p divide a y y p, lo que contradice que 1 sea el máximo común divisor. Por lo tanto, $y \in \mathbb{Z}^+ \setminus p\mathbb{Z}^+$.

Luego, si $y \in \mathbb{Z}^+ \setminus p\mathbb{Z}^+$, entonces para toda $k \in \mathbb{Z}^+$, $y \neq kp$. Así, p no puede dividir a y y como los únicos números que dividen a p son 1 y p, entonces tenemos que $\mathrm{MCD}(p,y) = 1$. ▲

[1] OJO: $\mathbb{Z}^+ \setminus p\mathbb{Z}^+$ es el complemento de $p\mathbb{Z}^+$ en $\mathbb{Z}^+$.

De esta manera, con la proposición anterior tenemos la siguiente cadena de igualdades:

$$\mathrm{Cop}_*(\mathbb{P}) = \bigcap_{p\in\mathbb{P}} \mathrm{Cop}_*(\{p\}) = \bigcap_{p\in\mathbb{P}} \mathbb{Z}^+ \setminus p\mathbb{Z}^+ = \mathbb{Z}^+ \setminus \bigcup_{p\in\mathbb{P}} p\mathbb{Z}^+.$$

Nuestra intuición y varios teoremas nos dicen que $\mathbb{Z}^+ \setminus \bigcup_{p\in\mathbb{P}} p\mathbb{Z}^+ = \{1\}$. En particular, con que sepamos que cada número entero tiene al menos un factor que es un número primo podemos concluir la igualdad $\mathbb{Z}^+ \setminus \bigcup_{p\in\mathbb{P}} p\mathbb{Z}^+ = \{1\}$.

Ahora ya sabemos que $\mathrm{Cop}_*(\mathbb{P})$ es finito solo con el hecho de saber que todo número tiene un factor primo. Para terminar demostramos el siguiente teorema, cuya transpuesta nos dira que $\mathbb{P}$ es infinito.

Teorema 2. Si $X \subseteq \mathbb{Z}^+$ es finito, entonces $\mathrm{Cop}_*(X)$ es infinito.

Demo: Como X es finito el mínimo común multiplo de X esta bien definido. Denotamos por $\mathrm{mcm}(X)$ tal número. Luego $\mathrm{mcm}(X)+1$ es coprimo con cada elemento de X. Aun más, para cada $n \in \mathbb{Z}^+$, $(\mathrm{mcm}(X)+1)^n$ es coprimo con cada elemento de X.

Si la última afirmación no es clara por inducción considere que $(\mathrm{mcm}(X)+1)^n$ es coprimo con $x \in X$. Entonces, si $z \in \mathbb{Z}^+$ es tal que $z \mid x$ y $z \mid (\mathrm{mcm}(X)+1)^{n+1}$ en particular existe $k \in \mathbb{Z}^+$ tal que $kz = x$. Así, $k \mid x$ y $x \mid k(\mathrm{mcm}(X)+1)^n(\mathrm{mcm}(X)+1)$, pero como x y $\mathrm{mcm}(X)+1$ son coprimos, debe pasar que $x \mid k(\mathrm{mcm}(X)+1)^n$. Por hipótesis de inducción, $(\mathrm{mcm}(X)+1)^n$ es coprimo con x, por lo tanto $x \mid k$.

De esta manera $x \mid k$ y $k \mid x$, lo que es equivalente a que $x = k$. Finalmente, como $kz = x$, concluimos que $z = 1$. Así, $\mathrm{MCD}(x, (\mathrm{mcm}(X)+1)^{n+1}) = 1$.

$\therefore \mathrm{Cop}_*(X)$ es infinito. ▲

De esta manera el teorema 1 es consecuencia inmediata del teorema anterior y como $\mathrm{Cop}_*(\mathbb{P}) = \{1\}$ podemos concluir que $\mathbb{P}$ es un conjunto infinito.