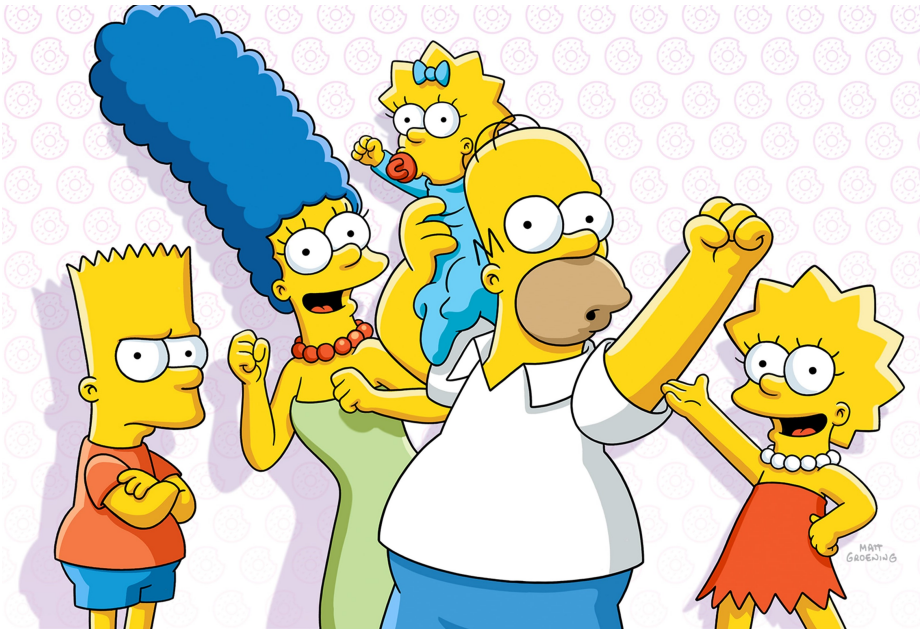
Los Simpsons

Grupo 1

Jon Pilarte, Andoni Latorre, Aitor Moreno,

Alberto Ruiz de Ázua, Mariana Zaballa, Mikel Navas

7 de Noviembre del 2020



1

Formula el último teorema de Fermat. Estudia brevemente la historia detrás del problema. ¿Por qué la fórmula en los Simpson contradice este teorema?

El teorema de Fermat dice que $\nexists a, b, c \in \mathbb{N} : a^n + b^n = c^n \quad \forall n \in \mathbb{N} - \{1, 2\}$.

Este teorema fue conjeturado por Pierre de Fermat en 1637, pero no fue demostrado hasta 1995 por Andrew Wiles ayudado por el matemático Richard Taylor. La búsqueda de una demostración estimuló el desarrollo de la teoría algebraica de números en el siglo XIX y la demostración del teorema de la modularidad en el siglo XX.

Aqui un resumen de la búsqueda de la demostración a este teorema.

Año	Acontecimiento
1665	Muere Fermat sin dejar constancia de su demostración.
1753	Leonhard Euler demostró el caso $n = 3$.
1825	Adrien-Marie Legendre demostró el caso para $n = 5$.
1839	Lamé demostró el caso n=7.
1843	Ernst Kummer afirma haber demostrado el teorema pero Dirichlet encuentra un error.
1995	Andrew Wiles publica la demostración del teorema.

Para probar que $1782^{12} + 1841^{12} = 1922^{12}$ no contradice el teorema veamos que es falso, para ello, trabajaremos módulo 2.
Por contradicción, asumiendo que es verdad, se tiene que:

$$\begin{aligned} 1782^{12} + 1841^{12} &\equiv 1922^{12} \pmod 2 \\ 0^{12} + 1^{12} &\equiv 0^{12} \\ 0 + 1 &\equiv 0 \\ 1 &\equiv 0 \end{aligned}$$

Lo cual es absurdo y concluye la prueba.

2

Resuelve cuántas maneras hay de poner un número natural n como suma de dos enteros que cumplan:

a. ambos pares y no negativos

Si $n \equiv 1 \pmod 2$, no hay soluciones. Si $n \equiv 0 \pmod 2$, las soluciones son:

$$n = 2k \quad k \in \mathbb{N}$$

x_1	x_2
$2 \cdot 0$	$2k$
$2 \cdot 1$	$2(k-1)$
$\vdots$	$\vdots$
$2 \cdot i$	$2(k-i)$
$\vdots$	$\vdots$
$2k$	0

que son $k+1$ soluciones.
Si $x_1^{(i)}, x_2^{(i)}$ s la solución iésima. Si $\begin{cases} x_1^{(i)} = x_2^{(j)} \\ x_2^{(i)} = x_1^{(j)} \end{cases}$, hay $\lceil \frac{k+1}{2} \rceil$ soluciones.

b. el primero par y el otro múltiplo de 3, ambos no negativos

Si $n \equiv 0 \pmod 2$, $n = 2k \quad k \in \mathbb{N}$. Las soluciones son:

x_1	x_2
$2 \cdot k$	$3 \cdot 2 \cdot 0$
$2k - 3 \cdot 2$	$3 \cdot 2 \cdot 1$
$\vdots$	$\vdots$
$2(k - 3i)$	$3 \cdot 2 \cdot i$
$\vdots$	$\vdots$
$2k - 3 \cdot 2\lfloor \frac{k}{3} \rfloor$	$3 \cdot 2\lfloor \frac{k}{3} \rfloor$

que son $\lfloor \frac{k}{3} \rfloor + 1$ soluciones. Si, $\begin{cases} x_1^{(i)} = x_2^{(j)} \\ x_2^{(i)} = x_1^{(j)} \end{cases}$ Hay $\left\lceil \frac{\lfloor \frac{k}{3} \rfloor + 1}{2} \right\rceil$ soluciones.

Si $n \equiv 1 \pmod 2$, $n = 2k+1 \quad k \in \mathbb{N}$. Las soluciones son:

x_1	x_2
$3 \cdot 1$	$2k + 1 - 3 \cdot 1 = 2k - 2$
$3 \cdot 3$	$2k + 1 - 3 \cdot 3 = 2k - 8$
$\vdots$	$\vdots$
$3(2i-1)$	$2k + 1 - 3(2i-1) = 2(k - 31 + 2)$
$\vdots$	$\vdots$
$3(2\lfloor \frac{k+4}{3} \rfloor - 3)$	$2(k - 3\lfloor \frac{k+4}{3} \rfloor + 5)$
$3(2\lfloor \frac{k+4}{3} \rfloor - 1)$	0

$$\left\lfloor \frac{k+4}{3} \right\rfloor = \left\lfloor \frac{k+1}{3} \right\rfloor + 1$$

c. ¿y si pudiesen ser negativos? Resolver a y b.

Para el caso de dos pares. De nuevo, si $n \equiv 1 \pmod 2$, no hay soluciones. En cambio, si $n \equiv 0 \pmod 2$, las soluciones son

x_1	x_2
$n+0$	0
$n+2$	-2
$\vdots$	$\vdots$
$n+2k$	$-2k$
$\vdots$	$\vdots$

} infinitas

Para el caso de uno par y el otro multiplo de tres:
Si $n \equiv 0 \pmod 2$ $n = 2k$ $k \in \mathbb{N}$

x_1	x_2
$\vdots$	$\vdots$
$2k + 3 \cdot 2 \cdot i$	$3 \cdot 2 \cdot -i$
$\vdots$	$\vdots$
$2k + 3 \cdot 2$	$3 \cdot 2 \cdot -1$
$2k$	$3 \cdot 2 \cdot 0$
$2k - 3 \cdot 2$	$3 \cdot 2 \cdot 1$
$\vdots$	$\vdots$
$2k - 3 \cdot 2 \cdot i$	$3 \cdot 2 \cdot i$
$\vdots$	$\vdots$

} infinitas

Si $n \equiv 1 \pmod 2$ $n = 2k + 1$ $k \in \mathbb{N}$

x_1	x_2
$\vdots$	$\vdots$
$3(-2i - 1)$	$2(k + 3i + 2)$
$\vdots$	$\vdots$
$3 \cdot -1$	$2k + 4$
$3 \cdot 1$	$2k - 2$
$3 \cdot 3$	$2k - 8$
$\vdots$	$\vdots$
$3(2i - 1)$	$2(k - 3i + 2)$
$\vdots$	$\vdots$

} infinitas

d. en cada uno de los casos, ¿cuántas formas hay de descomponer el número natural 12? ¿y el 1922?

	12	1922
a	7	962
b	2	321

3

Los números de Fermat son de la forma

$$f_n = 2^{2^n} + 1$$

Fermat conjeturó que todos esos números eran primos, pero años después Euler se encargó de refutar esa conjetura. Adivina el primer valor de n para el que f_n no es primo.

$$F_1 = 2^2 + 1 = 5 \rightarrow \text{primo}$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17 \rightarrow \text{primo}$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257 \quad \left\lfloor \sqrt{257} \right\rfloor = 25$$

$$2 \not| 257, 3 \not| 257, 5, 7, 11, 13, 17, 19, 23 \not| 257 \rightarrow \text{primo}$$

$$F_4 = 2^{2^4} + 1 = 2^16 + 1 = 65537 \quad \left\lfloor \sqrt{65537} \right\rfloor = 256$$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251 $\not|$ 65537

$$65537 \rightarrow \text{primo}$$

$$F_5 = 2^{2^5} + 1 = 2^32 + 1 = 4294967297$$

Usaremos el siguiente teorema de Euler,

La suma de dos números cuyos exponentes son múltiplos de 2, $a^{2^m} + b^{2^m}$, no admiten más divisores que aquellos de la forma $n \cdot 2^{m+1} + 1$.

Por lo tanto, $2^{2^5} + 1$, donde $m = 5$, sólo admite divisores de la forma $n \cdot 2^6 + 1 = n \cdot 64 + 1$, veamos,

$n = 1$	$64 \cdot 1 + 1 = 65$	$\rightarrow$	No es primo
$n = 2$	$64 \cdot 2 + 1 = 129$	$\rightarrow$	No es primo
$n = 3$	$64 \cdot 3 + 1 = 193$	$\rightarrow$	Es primo pero no divide a 4294967297
$n = 4$	$64 \cdot 4 + 1 = 257$	$\rightarrow$	Es primo pero no divide a 4294967297
$n = 5$	$64 \cdot 5 + 1 = 321$	$\rightarrow$	No es primo
$n = 6$	$64 \cdot 6 + 1 = 385$	$\rightarrow$	No es primo
$n = 7$	$64 \cdot 7 + 1 = 449$	$\rightarrow$	Es primo pero no divide a 4294967297
$n = 8$	$64 \cdot 8 + 1 = 513$	$\rightarrow$	No es primo
$n = 9$	$64 \cdot 9 + 1 = 577$	$\rightarrow$	Es primo pero no divide a 4294967297
$n = 10$	$64 \cdot 10 + 1 = 641$	$\rightarrow$	Es primo y divide a 4294967297 con cociente 6700417

el cual también es un número primo, $\lfloor \sqrt{6700417} \rfloor = 2588$ al que, por el teorema anterior, sólo pueden dividirlo números de la forma $64 \cdot n + 1$. Ya hemoos vsto los 10 primeros y, de los 30 restantes, sólo 6 de ellos son primos, $(769, 1153, 1217, 1409, 1601, 2113)$, pero ninguno divide a 2588.

4

Sin embargo, vamos a demostrar que el conjunto de números primos es infinito basándonos en esta familia de números. Veámoslo paso a paso:

a. Demuestra que todos son impares.

$$2^{2^n} + 1 \equiv 0^{2^n} + 1 \equiv 0 + 1 \equiv 1 \pmod 2$$

b. Demuestra la relación de recurrencia:

$$f_0 f_1 f_2 \cdots f_{n-1} = f_n - 2$$

Para demostrar esta relación de recurrencia lo haremos por inducción.

Primer probamos el caso base para n = 1:

$$f_0 = f_1 - 2$$

$$2^{2^0} + 1 = 2^1 + 1 = 3 = 5 - 2 = (4+1) - 2 = (2^2 + 1) - 2 = (2^{2^1} + 1) - 2$$

Ahora que sabemos que se cumple el caso base, utilizamos como hipótesis que se cumple para n-1 y probamos que se cumple para n.

$$f_0 f_1 f_2 \cdots f_{n-1} = f_n - 2$$

$$f_0 f_1 f_2 \cdots f_{n-1} f_n = (f_n - 2) f_n =$$

$${f_n}^2 + 2 f_n =$$

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

$$2^{2^{n+1}} \cancel{+ 2^{2^{n+1}}} + 1 \cancel{- 2^{2^{n+1}}} - 2 =$$

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

$$f_{n+1} - 2$$

c. Demuestra que ningún número de Fermat f_n es divisible por ninguno de los factores que forman los números de Fermat anteriores a él. Es decir, f_n es coprimo con $f_1, f_2, ..., f_{n-1}$.

$$f_n \equiv 0 \pmod{f_i} \quad 0 \leq i < n$$

$$f_n = \underbrace{f_0 f_1 f_2 \cdots f_i \cdots f_n}_{0} + 2 \equiv 0 \pmod{f_i}$$

$$f_n \equiv 2 \equiv 0 \pmod{f_i}$$

Como 2 es primo $f_i = 2$, lo cual es absurdo por *a)* y concluye la prueba.

d. Demuestra que el conjunto de los números primos es infinito, utilizando el resultado anterior.

Del apartado c se deduce que los números de Fermat son coprimos dos a dos. Por lo tanto cada número de Fermat tiene al menos un factor primo que no está presente en la factorización de cualquier otro número de Fermat. Al haber infinitos números de Fermat, hay infinitos primos.

5

¿Hay contradicción entre los dos ejercicios anteriores? ¿Por qué?

No, no hay contradicción, que exista un numero de Fermat que sea compuesto no impide que este sea coprimo con todos los demás números de Fermat.