DEFINICION DE TAOREMA Y SUS APLICACIONES A LA TEORIA DE NUMEROS

por

JOSE ANTONIO ESTRUGO

Se caracteriza la Teoría de Números por contener, además de los teoremas fundamentales que integran su propia doctrina, una profusión notable de proposiciones y conjeturas marginales, que no llegan a la categoría de teoremas; unas veces, por no haber sido hallada su demostración, y otras, porque al comprobar la verificación de la propiedad establecida vemos se cumple para determinados valores consecutivos de $n(n = 1, 2, 3 \ldots)$, pero falla en algunos otros, dándonos la sensación de tiempo perdido en la investigación, cuando, a nuestro entender, puede servir para dirigirla en otro sentido complementario.

Hemos de hacer resaltar que, precisamente esas proposiciones y conjeturas son las que han tenido y tienen más resonancia entre los matemáticos y aficionados, bien por incitar a su resolución el carácter desafiante que adquieren al no haber podido ser demostradas después de varios siglos de investigación, o también por el marcado interés que despiertan las ya resueltas, que han precisado utilizar los recursos más potentes del Análisis para doblegar la resistencia opuesta a la solución de proposiciones, cuyos enunciados parecían, en principio, muy sencillos.

Del extenso catálogo que pudiéramos citar de las primeras, destacamos el «último teorema de Fermat», demostrado para $n < 619$, pero no para todos los n y la famosa conjetura de Goldbach, propuesta a Euler, cuyos intentos de solución por Schnirelmann y posteriormente por Vinogradov, van acercándose al fin propuesto, sin haberlo aún conseguido. En cuanto a ejemplo de los recursos a emplear, señalamos el problema de la distribución de los números primos, que puede interpretarse mediante la función logarítmica, descubrimiento notable por ser sorprendente que dos conceptos matemáticos, al parecer tan dispares, estén de hecho íntimamente ligados.

Como cada propuesta o conjetura tiene un trato individual y, por tanto, independiente de la teoría constituida por los teoremas, creemos

justificado el crear una nueva definición, que al recoger todas ellas, el teorema quede comprendido como caso particular.

A estos efectos denominaremos TAOREMA (1) «a la expresión de una propiedad que se verifica *casi siempre,* aunque sus excepciones puedan ser infinitas, o bien no se hayan encontrado, pero se carece de una demostración general».

En el primer caso aparece una doble infinitud: la que representa el número de veces que al realizar las comprobaciones la propiedad se verifica, y el de aquellas en que no se cumple.

Se puede tratar desde un punto de vista estadístico las comprobaciones que se efectúen, calculando una frecuencia relativa aritmética entre el número de realizaciones de la propiedad indicada, n_r, y el total de las pruebas verificadas, n_c. Si el cociente

$$f_r = n_r/n_c$$

se observara que a medida que n_c aumenta, tiende a un número $p < 1$ entonces

$$f_r \to p$$

expresará la densidad asintótica aritmética de la propiedad objeto del Taorema, para $n_c \to \infty$.

Sin embargo, no será posible llevar muy lejos el estudio de la variación de la frecuencia aritmética, toda vez que, en general, aparecerán en los cálculos sucesivos números de gran valor absoluto, dificultando, si no impidiendo, las operaciones comprobatorias. Otras veces la densidad asintótica tenderá a cero. Así, por ejemplo, si denominamos A_n al número de primos existentes entre los n primeros números naturales, vemos que aunque $A_n \to \infty$, sin embargo, la relación $A_n/n \to 0$ (2).

Un Taorema cuya densidad asintótica sea de fácil cálculo carece —casi siempre— de interés. Por ejemplo, «La expresión n da siempre números impares». En este caso puede calcularse que $p = 1/2$ ($f_1 = 1$; $f_2 = 1/2$; $f_3 = 2/3$; $f_4 = 2/4$ ...).

Más interesante resultará —sin duda— encontrar una expresión funcional, exacta a ser posible, aproximada la mayoría de las veces, que permita escribir

$$f_r = n_r/n_c \sim f(n)$$

que nos servirá para obtener la medida del Taorema para valores superiores a los comprobados y, en su caso, el valor asintótico del mismo para $n_c \to \infty$.

El concepto de frecuencia relativa, aritmética o funcional nos lleva

---

(1) Hemos formado esta palabra, sustituyendo la *t* latina inicial por la *t* griega.

(2) La relación anterior correspondería a la frecuencia relativa del Taorema: «La expresión n ($n = 1, 2, \ldots$) da siempre números primos». Representando ahora A_n, el número de veces que se cumple y n el de comprobaciones realizadas.

a definirla como la probabilidad que tendríamos al verificar, al azar, una prueba cualquiera de las ya efectuadas. Por ejemplo, la $f_r = A_n/n$ nos señalará la probabilidad de que al elegir al azar un número menor que n, éste sea primo.

El caso particular en que

$$f_r = 1 \ (n_r = n_c = 1, 2, \ldots)$$

constituye el teorema, sustituyendo a las infinitas comprobaciones la demostración del mismo.

En el segundo caso, no siendo posible —por no existir demostración general— verificar las *infinitas* pruebas que se requieren para transformarlo en teorema, denominaremos tendencia a la unidad, denominador n_c, a dicha medida, que nos expresará hasta dónde han posido ser llevadas las comprobaciones (3). Esto es

$$f_r \to 1 \ (\text{den. } n_c)$$

Para distinguir el Taorema de un teorema mal enunciado, impondremos la condición de que si para ciertos valores de n la propiedad que constituye el Taorema falla, no por eso pierde *la tendencia* a seguir verificándose en los sucesivos.

Por ejemplo, si enunciamos como Taorema que «el polinomio de grado n, que resulte de desarrollar el producto

$$n\mathrm{P}(x) = \prod_{1}^{n} (x - k) = (x - 1)(x - 2) \ldots (x - n)$$

se anula para todos los valores de la serie natural», es evidente que esta propiedad se verificará para $x = 1, 2, 3, \ldots n$; pero a partir de este último número, el polinomio no se anulará para ningún otro valor entero superior a él; no constituyendo, por tanto, un Taorema.

El enunciado correcto, en virtud del teorema fundamental del Algebra, es el de que $n\mathrm{P}(x)$ se anula sólo para n valores, los que, debido a su construcción, coinciden con los n primeros números naturales.

Un Taorema tipo puede ser el siguiente:
«Todo número ciclotómico de orden p ($p > 1$),

$$\mu(p) = 10^{p-1} + 10^{p-2} + \ldots + 10 + 1 = 111 \ldots (p \ 1$$

admite una descomposición factorial en la que existen dos factores primos adjuntos, es decir, que tienen ambos el mismo número p de cifras de período» (4).

---

(3) No hace falta fijar el numerador, puesto que coinciden las realizaciones con n_c y su cociente sería la unidad, como si fuera un teorema. Por ello, introducimos *la tendencia a 1.*

(4) Haber considerado este enunciado como teorema para p primo, en un estudio que hicimos de este número, constituyó la idea para el presente trabajo. Le dimos dicha denominación por su parecido con la ecuación ciclotómica:

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

A este objeto construimos una tablilla en la que sólo indicamos los fatcores que interesan de $\mu(2)$ a $\mu(16)$:

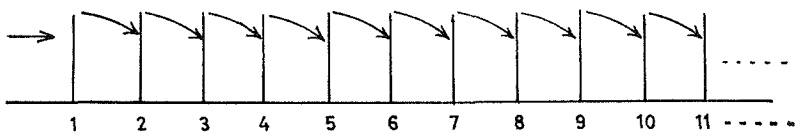
Orden p del ciclotómico	Factores primos que tienen p cifras de período	
2	11	primo aislado (5)
3	3 y 37	primos aislados (6)
4	101	primo aislado
5	41 y 271	
6	7 y 13	
7	239 y 4.649	
8	73 y 137	
9	333.667	primo aislado
10	9.091	primo aislado
11	21.649 y 513.239	
12	9.901	primo aislado
13	53; 79 y 265.371.653	(primos abundantes) (7)
14	909.091	primo aislado
15	31 y 2.906.161	
16	17 y 5.882.353	

Podemos observar que el Taorema no se cumple para $p = 2,3$ y 4; se verifica para $p = 5, 6, 7$ y 8; no se realiza para $p = 9$ y 10, y sí para $p = 11$; en $p = 12$, falla; para $p = 13$, ocurre lo mismo, por ser tres números los que la cumplen; para $p = 14$ no se verifica, cumpliéndose para $p = 15$ y 16.

La frecuencia relativa aritmética obtenida en las primeras quince pruebas realizadas es de $f_r = 7/15$.

Una representación gráfica que ponga de relieve la diferencia existente entre teorema y Taorema sería la siguiente, en donde las barras verticales podemos imaginar sean fichas de dominó.

(Teorema):



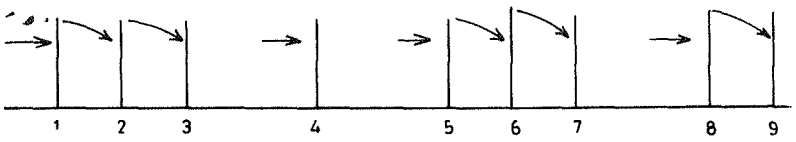
(5) Entendemos por «primo aislado» aquel cuyo número de cifras de período no comparte ningún otro.

(6) El 3 tiene una cifra de período y el 37, tres; luego ambos son primos aislados.

(7) «Primos abundantes», el caso en que sean más de dos los que tienen el mismo número de cifras de período.

La demostración del teorema nos garantiza que las fichas se encuentran a una distancia tal, que al empujar la primera caerán todas las restantes. (El teorema se cumple, pues, para $n = 1, 2, 3 \ldots \infty$.)

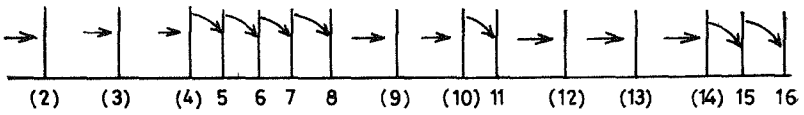
(Taorema):



Al empezar las comprobaciones (empujar las fichas) puede ocurrir incluso que las primeras no hagan caer las siguientes: en el ejemplo propuesto, la (1) puede o no realizarse, pero tira a la (2) y (3); la (4) no se realiza, ni la (5), pero ésta tira a la (6) y (7); no se cumple la (8) y s la (9).

Para concretar, hagamos la imagen gráfica del ejemplo propuesto como Taorema tipo; sería, encerrando entre paréntesis las que no cumplen la propiedad,

(Taorema tipo):



que no necesita explicación por el convenio establecido.

El hecho de que una ficha que no verifica la propiedad señalada tire a la siguiente, haciéndola cumplir, es lo que hemos denominado *tendencia*, que caracteriza al Taorema.

El principio de tendencia garantiza si existe un teorema al respecto, o al menos presume, si no se dispone de él, que existirán infinitas fichas, algunas incluso consecutivas, cuya distancia a la siguiente sea tal que, al empujar aquélla esta última caiga.

Si el recíproco de un teorema no es cierto, puede constituir un Taorema; como igualmente lo puede resultar toda condición necesaria, pero no suficiente, de una determinada propiedad.

Por ejemplo, enunciemos el siguiente teorema: «Todo número primo > 5 es de la forma $6k \pm 1$».

En efecto, escribamos

$$6n - 1,\ 6n,\ 6n + 1,\ 6n + 2,\ 6n + 3,\ 6n + 4;$$

para $n = 1, 2, 3, \ldots$, se obtiene la serie natural a partir de 5. Pero $6n$, $6n + 2$, $6n + 3$ y $6n + 4$ son pares ó $\dot{3}$, luego sólo pueden ser primos $6n - 1$, $6n + 1$, o ambos (8).

---

(8) El hecho de serlo ambos da lugar a los primos gemelos, es decir, que difieren en dos unidades.

Deducimos de lo anterior que todo número primo > 5 tiene que adoptar una cualquiera de las dos formas que expresa el teorema.

El recíproco no es cierto, puesto que existen infinitos números de la forma $6n \pm 1$ ($n = 1, 2, 3, \ldots$) que no son primos (9).

Por tanto, señalar la propiedad «Todos los números de expresión $6n \pm 1$ ($n = 1, 2, \ldots$) son primos» es un Taorema.

El presente Taorema merece ser estudiado con algún detenimiento.

En primer lugar, el *principio de tendencia* está garantizado por el teorema de Euclides (existen infinitos números primos).

Es posible hallar la frecuencia relativa aritmética y funcional, ya que si A_n representa el número de primos inferiores a n, en la actualidad se conoce que para

$$n = 10^3 \text{ , } A_n = 168$$
$$n = 10^6 \text{ , } A_n = 78.498$$
$$n = 10^9 \text{ , } A_n = 50.847.478$$

así como la relación asintótica

$$A_n/n = 1/ln\,(\alpha)$$

El número de comprobaciones a realizar de números de la forma $6n \pm 1$, dentro de los 10^m primeros números es

$$\frac{10^m - 4}{3};$$

por tanto, tendremos las siguientes frecuencias relativas

$$f_r(10^3) = \frac{166}{\frac{10^3\text{-}4}{3}} = \frac{498}{10^3\text{-}4} = 0{,}5$$

$$f_r(10^6) = \frac{78.496}{\frac{10^6\text{-}4}{3}} = \frac{235.488}{10^6\text{-}4} = 0{,}2355$$

$$f_r(10^9) = \frac{50.847.476}{\frac{10^9\text{-}4}{3}} = \frac{152.542.428}{10^9\text{-}4} = 0{,}1525$$

---

(9) Por ejemplo, todos los números de la forma:

$6(5k \pm 1) \mp 1 = \dot{5}$; $6(7k \mp 1) \mp 1 = \dot{7}$; $6(11k \mp 2) \pm 1 = \dot{11}$; etc.

($k = 0, 1, 2 \ldots$)

Y de la relación asintótica (α) podemos expresar la frecuencia relativa funcional de más importancia

$$f_r(n) = \frac{3n}{(n + 2)ln}$$

incluyendo ahora como comprobaciones las que dan los dos primeros primos, 2 y 3, no tenidos en cuenta anteriormente.

Puede observarse que pese a la apariencia perfecta del Taorema, el límite asintótico es $f_r(n) = 0$.

Para nosotros el Taorema tipo sería aquel en que $\lim f_r(n) = p$ $(0 < p < 1)$, ya que expresaría el paso, de todo punto importante, de la frecuencia relativa aritmética, a la funcional, pudiendo señalarse el valor de p como medida asintótica del Taorema.

Si en lugar de indicar una propiedad numérica, lo que expresamos es un suceso estocástico, por ejemplo, «Al lanzar un dado aparece siempre el punto 2» (10), constituye desde otro punto de vista un Taorema, en donde las comprobaciones son los sucesivos lanzamientos que realicemos, siendo objeto del Cálculo de Probabilidades la obtención de la densidad asintótica. En este caso se mantiene el principio de tendencia, por el hecho de que, en cada una de las tiradas que se efectúen, se encuentra el punto 2, y el valor límite que se obtendría, razonado «a priori» o experimentalmente, $p = 1/6$, nos daría la medida de la densidad asintótica o probabilidad del Taorema.

En otros casos, la proyección de la definición de Taorema fuera de la Teoría de Números podría dar lugar a *Taoremas sin medidas*. Por ejemplo, si señalamos «Toda serie cuyo término general $u_n \to 0$, es convergente» resulta un Taorema, ya que existen infinitas series que, cumpliendo esta condición, son divergentes. Se ve fácilmente que la medida de este Taorema no se adaptaría a la sistemática seguida en el presente trabajo.

De todo lo anterior se deduce que la introducción del concepto de Taorema en la Matemática, la transformaría en un conjunto total de afirmaciones no vacías, la mayoría de las cuales, mediante un razonamiento lógico, es posible evidenciar su certeza (Teoremas), y el resto, o se cumplen, pero se carece de una demostración general, o se verifican parcialmente infinitas veces (Taoremas); y también, que a cada afirmación —salvo determinados Taoremas— se le puede asignar un número p $(0 \leq p \leq 1)$, que nos exprese su medida objetiva.

---

(10) Este enunciado es la expresión, en forma de Taorema, de su equivalente: «Probabilidad de que al lanzar un dado aparezca el punto 2».