CINCO PRUEBAS PARA UN TEOREMA DE EUCLIDES

O.A. Campoli

El teorema de Euclides a que hace referencia el título de ésta nota es el que afirma que el conjunto de los números naturales primos es un conjunto infinito.

De las cinco demostraciones que se mencionan, la más conocida es cronológicamente la primera. Se debe a Euclides mismo y es la más elemental y corta de las cinco.

El interés de las cinco demostraciones que daremos está en que las cinco usan razonamientos muy diferentes y dos de entre ellas al menos (la primera y la tercera) han tenido consecuencias importantes que trataremos de poner de manifiesto en cada caso.

Las tres primeras están ordenadas de acuerdo a su creciente orden de complejidad, que no coincide con su orden de aparición. Las dos últimas me fueron comunicadas recientemente por E.R. Gentile a través de C.U. Sanchez y usan solo algunos hechos elementales de divisibilidad que aclaramos en cada caso.

Primera prueba

Esta prueba usa sólo el hecho de que todo número natural mayor que 1 tiene un divisor primo.

Este hecho es muy fácil de ver por un argumento inductivo. En efecto, si n es un número natural mayor que 1 entonces n es primo o no lo es. Si n es primo entonces n es un divisor primo de n y se acabó el argumento.

Si n no es primo entonces $n = p.q$ con p, q naturales mayores que 1 y menores que n. Luego p es primo ó ... etc.

Para hacer la demostración de Euclides, usamos un argumento por el absurdo.

Supongamos que el conjunto de todos los números naturales primos fuese un conjunto finito. Digamos entonces que $p_1, p_2, \ldots, p_r$ son todos sus elementos.

Nos fijamos a continuación en el número $n = p_1 . p_2 \ldots p_r + 1$

Por ser n un natural mayor que 1 debe tener un divisor primo. Este divisor primo debe ser entonces uno entre $p_1, p_2, \ldots, p_r$. Digamos entonces que p_j divide a n. Como p_j ciertamente divide a $p_1 . p_2 \ldots p_r$

sigue que p_j debe dividir a 1.

Esto es absurdo y provino de suponer que el conjunto $\mathcal{P}$ de todos los números naturales primos era finito. Esto concluye la demostración del teorema.

A modo de comentario digamos que el argumento de esta demostración, además de ser el primero y más simple de los que llevan al teorema de Euclides, tuvo otras consecuencias inmediatas y mediatas. Mencionamos las inmediatas a continuación y dejamos las otras para el final de la tercera prueba.

En efecto, usando argumentos muy parecidos uno puede fácilmente probar que no solo $\mathcal{P}$ es un conjunto infinito sino que el subconjunto de $\mathcal{P}$ de los elementos de la forma $4n + 3$, para algún natural n, es también un conjunto infinito.

Esto se expresa usualmente diciendo que el conjunto de los naturales primos congruentes a 3 módulos 4 es un conjunto infinito.

Análogamente se puede probar que hay una infinidad de números primos de la forma $6n + 5$ y algunos otros ejemplos más.

Segunda prueba

Esta prueba es cronológicamente la última de las tres primeras que daremos y se debe a G. Polya, un matemático contemporáneo.

La demostración es *"constructiva"* en el sentido de que consiste en dar una familia infinita de números naturales coprimos dos a dos.

Usando de nuevo que todo número natural tiene un divisor primo, la existencia de una tal familia claramente implica que hay una infinidad de números primos ya que probamos que el conjunto de los divisores primos de los números de la familia es ya infinito.

Pasamos entonces a definir la familia mencionada y a probar sus propiedades.

Para cada número natural n, ponemos

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

A f_n se lo llama el n-ésimo número de Fermat y si es primo se dice que es un primo de Fermat.

Tenemos por ejemplo que

$$f_1 = 2^2 + 1 = 5$$

$$f_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$$

$$f_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$

$$f_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$$

Estos primeros cuatro números calculó Fermat y vio que eran primos. Conjeturó entonces que todos los siguientes eran también primos lo que obviamente implicaría el teorema de Euclides.

Esta conjetura fue hallada falsa por Euler al probar que $f_5 = 2^{32} + 1$ tiene a 641 por divisor (es decir, f_5 no es primo).

A partir de Euler, todos los cálculos de sucesivos números de Fermat han dado como resultado un número compuesto (es decir, no primo) y parece afianzarse la nueva conjetura de que los primos de Fermat forman un conjunto finito.

En éste sentido uno podría decir que la conjetura de Fermat no fue muy feliz. Sin embargo, a pesar de no ser todos primos, los números de Fermat tienen otra propiedad más débil pero que también implica el teorema de Euclides: es una familia de números coprimos dos a dos.

Para probar ésto, probamos primero que si $m > n$ entonces f_n divide a $f_m - 2$.

En efecto, digamos que $m = n + k$, k natural.

Llamemos $a = 2^{2^n}$. Entonces

$$\frac{f_m - 2}{f_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{\left(2^{2^n}\right)^{2^k} - 1}{2^{2^n} + 1} = \frac{a^{2^k} - 1}{a + 1} =$$

$$= a^{2^k - 1} - a^{2^k - 2} + \ldots + a^{2^k - (2^k - 1)} - a^0$$

lo que es claramente un número entero y hemos así probado que si $m > n$ entonces f_n divide a $f_m - 2$.

Veamos entonces ahora que si $m \neq n$ entonces f_m y f_n son coprimos.

Digamos que $m > n$.

Supongamos, por el absurdo, que f_m y f_n tienen un divisor primo común p. Como p divide a f_n, debe dividir a $f_m - 2$ y como divide a f_m también, debe dividir a 2.

Como f_m es impar, p no puede ser 2 y como 2 es primo, p debe ser

1. Absurdo.

Hemos probado entonces que si $m > n$ f_m y f_n, son coprimos y ésto concluye la segunda prueba del teorema de Euclides.

Tercera prueba

Esta prueba es la que envuelve los razonamientos más complicados entre las cinco que daremos.

Es a su vez la que ha tenido más consecuencias al constituirse en uno de los orígenes de lo que actualmente se llama teoría analítica de números.

La prueba conduce a la demostración de un hecho mucho más fuerte aún que la afirmación original de Euclides. Pasamos a aclarar ésta última afirmación.

Lo que probaremos es que los números primos no sólo forman un conjunto infinito sino que además, sumando los recíprocos de números primos podemos obtener un número tan grande como se quiera. Esto lo expresamos diciendo que la serie de los recíprocos de los números naturales primos es divergente y lo escribimos

$$\sum_{p \text{ primo}} \frac{1}{p} = \infty$$

Decimos que ésta afirmación es más fuerte que el teorema de Euclides porque obviamente lo tiene por consecuencia pero además, si nos fijamos por ejemplo en el conjunto formado por los números $2, 4, 8, 16, \ldots, 2^n, \ldots$, vemos que es un conjunto infinito. Sin embargo, uno puede fácilmente convencerse que cualquier suma de los recíprocos de un subconjunto de entre ellos es menor o igual que 1.

En símbolos

$$\sum_{n \text{ natural}} \frac{1}{2^n} \leq 1$$

En realidad se puede ver que con la definición apropiada de suma de un número infinito de sumandos se tiene

$$\sum_{n \text{ natural}} \frac{1}{2^n} = 1$$

El hecho de que $\sum_{p \text{ primo}} \frac{1}{p} = \infty$ está entonces expresando que los números naturales primos no sólo son infinitos sino que además no están *"crecientemente espaciados"* en su aparición entre los sucesivos números naturales.

Pasamos a la demostración de los hechos mencionados no sin antes aclarar que suponemos conocida la definición de convergencia de una serie de números positivos y el teorema fundamental de la aritmética que dice que todo número natural mayor que 1 posee una factorización única como producto de números primos (única salvo reordenamiento).

Digamos que $p_1 = 2$, $p_2 = 3, \ldots,$ p_j son los primeros j números primos.

Para cada número natural a, llamemos $N_j(a)$ a la cantidad de números naturales menores o iguales que a y que no son divisibles por números primos mayores que p_j.

Notemos entonces que si el teorema de Euclides fuese falso y $p_1, p_2, \ldots, p_j$ fuese la lista completa de los números primos tendríamos que

$$N_j(a) = a$$

cualquiera sea el número natural a.

La primera afirmación que queremos probar acerca del número $N_j(a)$ es que

(I) $$N_j(a) \leq 2^j \sqrt{a}$$

Si probamos la afirmación (I), con lo notado antes tendríamos otra demostración del teorema de Euclides ya que si $p_1, p_2, \ldots, p_j$ fuese la lista completa de los números primos tendríamos que para cualquier número natural a se debería cumplir

$$a = N_j(a) \leq 2^j \sqrt{a}$$

y ésto es claramente falso con sólo tomar $a = 2^{2j+2}$.

Para probar la afirmación (I) queremos contar los números naturales menores o iguales que a, que no son divisibles por números primos mayores que p_j. Digamos entonces que n es un tal natural.

Podemos escribir entonces

$$n = n_1^2 . m$$

donde $m = 2^{r_1} 3^{r_2} \ldots p_j^{r_j}$ y los números $r_1, r_2, \ldots, r_j$ toman

los valores 0 ó 1 solamente.

Es decir, hemos descompuesto n en producto de un número natural al cuadrado y un número que no es divisible por el cuadrado de un número primo. Por supuesto que tanto n_1 como m tienen a 1 como valor posible de acuerdo al n que hayamos elegido. Al expresar m como producto de primos hemos usado la hipótesis sobre n de no tener divisores primos mayores que p_j.

Debido a las posibilidades de los exponentes r_1, r_2, ..., r_j sigue entonces que la cantidad de valores posibles para m es menor o igual que 2^j.

Por otra parte al ser $n_1 \leq \sqrt{n} \leq \sqrt{a}$ sigue entonces que la cantidad de valores posibles para n_1 es a su vez menor o igual que $\sqrt{a}$.

Estas dos afirmaciones prueban la validez de la desigualdad (I).

Pasamos a continuación a probar la divergencia de la serie de los recíprocos de los números primos.

Digamos como arriba que p_j es el j-ésimo número primo (ya hemos destacado que de la validez de (I) sigue la validez del teorema de Euclides).

Si suponemos por el absurdo que la serie no es divergente, sigue de ésto que podemos hallar un número natural j tal que la suma de los recíprocos de todos los números primos mayores que p_j es menor que 1/2. En símbolos

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \ldots < \frac{1}{2}$$

Observemos ahora que dado un número natural a y un número primo p, el conjunto de los números naturales menores o iguales que a que son divisibles por p tiene una cantidad menor o igual que a/p de elementos.

Luego como $a - N_j(a)$ es exactamente la cantidad de elementos del conjunto de números naturales menores o iguales que a y que son divisibles por algún primo mayor que p_j, sigue de la observación anterior que debemos tener

$$a - N_j(a) \leq \frac{a}{p_{j+1}} + \frac{a}{p_{j+2}} + \cdots \leq \frac{a}{2}$$

Pasando de miembros entre el primero y el tercero obtenemos

$$\frac{a}{2} \leq N_j(a)$$

y como ya teníamos

$$N_j(a) \leq 2^j \sqrt{a}$$

sigue que

$$\frac{a}{2} \leq 2^j \sqrt{a}$$

o lo que es lo mismo

$$a \leq 2^{j+1} \sqrt{a}$$

Esto es otra vez una afirmación falsa con sólo tomar

$$a > 2^{j+2}$$

Este absurdo concluye la demostración de la divergencia de la serie de los recíprocos de los números primos.

A modo de comentario podemos agregar que la divergencia de ésta serie es sólo un caso particular de un teorema de Dirichlet que afirma que es divergente la serie de los recíprocos de los naturales primos congruentes a b módulo a, para cualquier par a,b de naturales coprimos. (Un entero x se dice congruente a b módulo a si existe otro entero k tal que $x = ka + b$. En éste caso se escribe $x \equiv b$ (mód. a)).

Es decir la afirmación que recién probamos es el caso $a = b = 1$ del teorema de Dirichlet.

La primera prueba del teorema de Euclides y las consecuencias que mencionamos en su caso, daban ya algunos ejemplos del hecho de que hay una infinidad de números primos congruentes a b módulo a si a y b son coprimos. Podría entonces decirse que el teorema de Dirichlet es una consecuencia de la primera y tercera pruebas del teorema de Euclides.

Digamos además que todo lo expuesto arriba puede hallarse, por ejemplo, en el libro "An Introduction to the Theory of Numbers" de G.H. Hardy y E.M. Wright.

Allí pueden hallarse también muchas más referencias, comentarios y notas históricas.

Cuarta prueba

Esta prueba consiste en ver que si p es un número primo entonces cualquier divisor primo del número $2^p - 1$ es mayor que p.

Esto implica la validez del teorema de Euclides ya que no puede existir un *"último"* número primo.

Para mostrar la afirmación mencionada, necesitamos recordar algunos hechos elementales de divisibilidad.

La fórmula del binomio de Newton dice que si n es un natural cualquiera

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

donde los números $\binom{n}{k}$ se definen de la siguiente manera

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{1.2.3\ldots.k.} \quad , \quad 0 \leq k \leq n$$

Mirando la definición del número $\binom{n}{k}$ uno puede convencerse del hecho de que si p es un número primo y k es un número natural tal que $1 \leq k < p$, entonces el número $\binom{p}{k}$ es divisible por p ya que p aparece en la factorización del numerador y no en la del denominador de $\binom{p}{k}$.

Entonces el primer resultado de divisibilidad que queríamos recordar es que si p es un número primo entonces p divide a $\binom{p}{k}$ para $0 < k < p$, lo que también se escribe

$$\binom{p}{k} \equiv 0 \text{ (mód. } p) \quad , \quad 0 < k < p$$

cualquiera sea el número primo p.

Ahora, si a y b son números enteros y p es un número primo, tenemos

$$(a + b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

Luego de lo anterior sigue que p divide al número $(a + b)^p - a^p - b^p$, esto es

$$(a + b)^p \equiv a^p + b^p \text{ (mód. } p)$$

Usando éste hecho y un argumento muy simple de inducción en n, se

puede ver que cualquiera sea el natural n y el primo p se tiene que p divide $n^p - n$.

De éste último hecho sigue el llamado teorema de Fermat que dice que si p es primo y n no es divisible por p entonces p divide a $n^{p-1} - 1$ ya que p divide a $n(n^{p-1} - 1) = n^p - n$ y no divide a n.

Con estos resultados podemos probar la afirmación mencionada al comienzo: si p es primo entonces cualquier divisor primo de $2^p - 1$ es mayor que p.

En efecto, podemos suponer que $2^p - 1$ no es primo ya que en caso de serlo nuestra afirmación es claramente cierta.

Sea entonces q un divisor primo de $2^p - 1$.

Queremos ver que $q > p$.

Como q divide a $2^p - 1$ podemos considerar el mínimo entre todos los números naturales n tales que q divide a $2^n - 1$ y llamarlo t. Es decir, q divide a $2^t - 1$ y si q divide a $2^n - 1$ para algún natural n, entonces $t \leq n$. En particular entonces se tiene que $t \leq p$.

Veamos que $t = p$.

Si tuviéramos por el contrario que $t < p$ entonces como q divide a $2^p - 1$ y también a $2^t - 1$ se sigue que q divide a $2^p - 1 - (2^t - 1) = 2^p - 2^t = 2^t(2^{p-t} - 1)$ y como q es impar debe dividir a $2^{p-t} - 1$.

Repitiendo éste razonamiento llegamos a la conclusión de que existe un entero k tal que $2^{p-kt} - 1 = 2^t - 1$ de donde sigue que

$$p - kt = t$$

y finalmente que

$$p = (k + 1)t$$

Usando ahora que p es primo y $t > 1$ sigue que $k + 1 = 1$ y luego que $p = t$.

Ahora como q es impar, el teorema de Fermat dice que q divide a $2^{q-1} - 1$ y entonces por lo que acabamos de ver sigue que $p \leq q - 1$ de donde sigue la conclusión buscada, esto es

$$p < q$$

Quinta prueba

Esta última prueba que daremos del teorema de Euclides consiste en un razonamiento por el absurdo usando un teorema que se conoce con el nombre de teorema chino del resto y procede como sigue.

Supongamos que p_1 , p_2 ,..., p_n fuesen todos los números naturales primos impares.

El teorema chino del resto (que a continuación justificamos) asegura que existe un número entero a tal que:

$$\begin{aligned} 2 &\text{ divide a } a + 1 \\ p_1 &\text{ divide a } a + 1 \\ p_2 &\text{ divide a } a - 1 \\ p_3 &\text{ divide a } a - 1 \\ &\vdots \\ p_n &\text{ divide a } a - 1 \end{aligned}$$

De ésto sigue que ningún número primo divide a a . Entonces

$$a = 1 \quad \text{ó} \quad a = -1 .$$

Pero si fuese $a = 1$, la segunda condición impuesta en a por el teorema chino dice que 3 divide a 2 , lo que es absurdo.

Análogamente, si fuese $a = -1$, la tercera condición diría que 5 divide $a - 2$ lo que también es un absurdo.

Luego la negación del teorema de Euclides lleva a la negación del teorema chino del resto.

Pasamos entonces a justificar el teorema chino del resto.

La afirmación que queremos probar dice que si m_1 , m_2 ,..., m_r son números naturales coprimos dos a dos y a_1 , a_2 ,..., a_r son números enteros cualesquiera, entonces existe un número entero x tal que

$$\begin{aligned} m_1 &\text{ divide a } x - a_1 \\ m_2 &\text{ divide a } x - a_2 \\ &\vdots \\ m_r &\text{ divide a } x - a_r \end{aligned}$$

(Hemos usado ésta afirmación en el caso $m_1 = 2$, $m_2 = p_1$,..., $m_r = p_n$ y $a_1 = -1$, $a_2 = -1$, $a_3 = 1$,..., $a_r = 1$).

Hacemos la demostración para el caso $r = 3$ ya que, creemos, su prueba ilustra claramente el caso general.

Sabiendo entonces que m_1 , m_2 , m_3 son números coprimos dos a

dos quisiéramos hallar un número entero x , tal que m_1 divide a $x - a_1$, m_2 divide a $x - a_2$ y m_3 divide a $x - a_3$.

Para ello notamos que es suficiente saber que podemos hallar números enteros x_1 , x_2 , x_3 tales que

m_1 divide a $x_1 - 1$, a x_2 y a x_3
m_2 divide a x_1 , a $x_2 - 1$ y a x_3
m_3 divide a x_1 , a x_2 y a $x_3 - 1$

ya que en éste caso, el número

$$x = a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_3$$

satisface todas las propiedades requeridas.

Demos a modo de ejemplo, la forma de hallar x_1 . Un procedimiento totalmente análogo nos daría x_2 y x_3 .

De x_1 se requiere que m_1 divida a $x_1 - 1$, m_2 divida a x_1 y m_3 divida á x_1 .

Ahora, si k es un entero cualquiera, el número $k.m_2.m_3$ satisface los dos últimos requerimientos. Luego, bastaría encontrar un valor de k que también satisfaga el primero.

La hipótesis sobre m_1 , m_2 , m_3 asegura que m_1 y $m_2.m_3$ son números coprimos y ésto dice que existen números enteros k y r tales que

$$1 = k\, m_2.m_3 + r\, m_1$$

Está claro entonces que éste k es el que buscamos.

Para concluir quisiéramos dejar un par de ejercicios, algunos de los cuales tienen relación con afirmaciones hechas en el texto de la nota.

1) Sea $2, 3, 5, \ldots, p$ la lista de los primos menores o iguales que p . Sea $q = 2.\ 3.\ 5 \ldots\ p$.
   Mostrar que $q + 2$, $q + 3$, $\ldots$, $q + p$ son todos números compuestos.
2) Usando un razonamiento como en la primera prueba del teorema de Euclides, mostrar que hay infinitos primos de la forma $4n + 3$.
3) Si a es un natural mayor o igual que 2 y $a^n + 1$ es un número primo entonces $n = 2^m$ para algún m .
4) Si $n > 1$ y $a^n - 1$ es un número primo entonces $a = 2$ y n es primo.
5) Sea n un número natural, $p_1, \ldots, p_s$ naturales primos, $r_1, \ldots, r_s$ enteros no negativos.
   La antidad de números de la forma $p_1^{r_1} \ldots p_s^{r_s}$ que son menores

o iguales que n es a su vez menor o igual que

$$\left(1 + \frac{\log n}{\log p_1}\right)\left(1 + \frac{\log n}{\log p_2}\right) \cdots \left(1 + \frac{\log n}{\log p_s}\right) \cdots$$

Usando éste hecho y el hecho de que cualquiera sea el natural r se tiene

$$\lim_{n \to \infty} \frac{(\log n)^r}{n} = 0$$

se puede obtener una sexta demostración del teorema de Euclides.

6) Si p es un antural primo y a, b son enteros tales que $p^2 = a^2 + b^2$, entonces p es de la forma $4k + 1$, i.e., es congruente a 1 módulo 4.

$$4.1 + 1 = 5 = 2^2 + 1^2$$
$$4.3 + 1 = 13 = 3^2 + 2^2$$
etc.

Vale también que si p es un natural primo tal que 4 divide a $p - 1$ entonces existen enteros a y b tales que $p = a^2 + b^2$ y que existen infinitos primos de ésta forma. Sin embargo ambas cosas son un poco más difícil de probar.

Instituto de Matemática, Astronomía y Física

Universidad Nacional de Córdoba