Un caso particular del teorema de Dirichlet

Juan Sabia[1] - *Susana Tesauri*[2]

1 Introducción

Uno de los problemas clásicos en Teoría de Números es la ubicación de los números primos en el conjunto de los números naturales. El teorema de Dirichlet (1837) establece que, si a y n son números naturales coprimos, hay infinitos primos en la sucesión $n + a$, $2n + a$, $3n + a$, $\cdots$. Las demostraciones conocidas de este teorema son difíciles: la prueba original de Dirichlet usa teoría analítica de números y hay otras posteriores, más algebraicas, de Selberg ([7]) y de Zassenhaus ([10]), por ejemplo.

En algunos casos particulares, hay demostraciones de este teorema más elementales. Por ejemplo, la primera demostración conocida de la infinitud de números primos, que se encuentra en los Elementos de Euclides (siglo III a. C.), puede pensarse como un caso particular de este teorema para $a = n = 1$. Otro caso similar es la siguiente demostración elemental de la infinitud de primos de la forma $4k + 3$ con $k \in \mathbb{N}$: Si, además del 3, hubiese finitos primos $p_1, \ldots, p_r$ de esta forma (este conjunto no es vacío porque el 7 es uno de estos primos), consideremos $m = 4.p_1.\cdots.p_r + 3$. Como el número impar m no es divisible por 3 ni por ninguno de los p_i $(1 \leq i \leq r)$, cualquier primo que divida a m debe ser de la forma $4h + 1$ para $h \in \mathbb{N}$. Luego

$$3 \equiv m \equiv (4h_1 + 1).(4h_2 + 1).\cdots.(4h_t + 1) \equiv 1 \text{ (mód 4)}$$

lo que es un absurdo que provino de suponer que había finitos primos de la forma $4k + 3$. Una demostración similar puede usarse para probar que hay infinitos primos de la forma $6k + 5$.

Para el caso particular $a = 1$, existen distintas demostraciones elementales del Teorema de Dirichlet (ver, por ejemplo, [2, 4, 5, 6, 8, 9])

En lo que sigue, daremos una demostración del Teorema de Dirichlet para el caso $a = 1$ que sólo usa aritmética elemental, polinomios en una variable y raíces de la unidad.

2 Un resultado aritmético

En esta sección, demostraremos un resultado auxiliar de divisibilidad entre números naturales que vamos a necesitar más adelante. Antes de este resultado, veamos que ciertas cuentas pueden hacerse módulo un primo.

Sea $p \in \mathbb{N}$ un número primo, y sea $b \in \mathbb{Z}$ coprimo con p. Entonces, la ecuación de congruencia $b.X \equiv 1$ (mód p) tiene una única solución c tal que $1 \leq$

[1]Parcialmente financiado por el subsidio CONICET PIP 5852/05
[2]Parcialmente financiado por el subsidio UBACyT X847 (2006-2009)

$c \leq p-1$. A esta solución la llamaremos b^{-1}, ya que es el inverso multiplicativo de b módulo p. Esto nos permite definir, para $b \in \mathbb{Z}$ coprimo con p, b^r módulo p para cualquier $r \in Z$:

$$b^r \equiv \begin{cases} b^r \pmod{p} & \text{si } r \geq 0 \\ (b^{-1})^{-r} \pmod{p} & \text{si } r < 0 \end{cases}$$

Con esta definición, es fácil probar las siguientes congruencias módulo p, cuando $b \in \mathbb{Z}$ es coprimo con p y $r, s \in \mathbb{Z}$:

$$\begin{array}{c} b^{r+s} \equiv b^r.b^s \pmod{p} \\ b^{r.s} \equiv (b^r)^s \pmod{p} \end{array} \tag{1}$$

Usando esta propiedad, vamos a demostrar el siguiente

Lema 2.1 *Sean $n, b \in \mathbb{N}$. Si $p \in \mathbb{N}$ es un número primo tal que $p \mid b^n - 1$ y $p \nmid b^d - 1$ para todo $d < n$ divisor positivo de n, entonces $n \mid p - 1$.*

Demostración. Como $p \mid b^n - 1$, es claro que p es coprimo con b, ya que de lo contrario, p dividiría a 1. Usando el pequeño teorema de Fermat, tenemos que $b^{p-1} \equiv 1 \pmod{p}$. Sea $M = (n, p-1)$ el máximo común divisor entre n y $p-1$. Entonces, existen enteros r, s tales que $M = n.r + (p-1).s$. Como $(b, p) = 1$ y $r, s \in \mathbb{Z}$, usando (1),

$$b^M = b^{r.n+s.(p-1)} = (b^n)^r.(b^{p-1})^s \equiv 1 \pmod{p}.$$

Luego, M es un divisor de n tal que $p \mid b^M - 1$. Entonces, por nuestra hipótesis, $M = n$, con lo que $n \mid p - 1$. □

Este lema nos da una herramienta para encontrar primos p tales que $p \equiv 1 \pmod{n}$. En la siguiente sección, introduciremos algunas nociones de polinomios que nos permitirán encontrar primos que cumplan estas condiciones.

3 Polinomios ciclotómicos

Sea $n \in \mathbb{N}$. Recordemos que una raíz n-ésima de la unidad es cualquiera de los n números complejos distintos que son raíces del polinomio $X^n - 1$. Una raíz n-ésima *primitiva* de la unidad ξ es una raíz n-ésima de la unidad tal que cualquier potencia positiva más chica que n no da 1, es decir

$$\xi^d \neq 1 \text{ para todo } 1 \leq d < n.$$

Cada ξ raíz n-ésima de 1 debe ser d-ésima primitiva para algún d único tal que $1 \leq d \leq n$. Más aún, d resulta un divisor de n, ya que si $M = (n, d)$,

escribiéndolo como combinación lineal de n y d, se tiene que $\xi^M = 1$ y por lo tanto $d = M$. Luego,

$$\{\xi \in \mathbb{C} \mid \xi^n = 1\} = \bigcup_{d\in\mathbb{N},\, d|n} \{\xi \in \mathbb{C} \mid \xi \text{ es raíz primitiva } d-\text{ésima de } 1\} \qquad (2)$$

donde la unión de la derecha es disjunta.

Definición 3.1 *Dado $n \in \mathbb{N}$, se llama* polinomio ciclotómico de índice n *al polinomio $\Phi_n(X) \in \mathbb{C}[X]$ definido por*

$$\Phi_n(X) := \prod_{\xi \text{ raíz primitiva } n\text{-ésima de } 1} (X - \xi).$$

Notar que, de (2), se tiene que

$$X^n - 1 = \prod_{d\in\mathbb{N},\, d|n} \Phi_d(X). \qquad (3)$$

La siguiente propiedad de los polinomios ciclotómicos se basa en que si un polinomio con coeficientes enteros es divisible en $\mathbb{C}[X]$ por un polinomio mónico con coeficientes enteros, entonces el cociente resulta tener coeficientes enteros, lo que es evidente a partir del algoritmo recursivo clásico de división de polinomios.

Lema 3.2 *Para todo $n \in \mathbb{N}$, el polinomio ciclotómico $\Phi_n(X)$ tiene coeficientes enteros.*

Demostración. Lo demostraremos por inducción global en n. Si $n = 1$, $\Phi_1(X) = X - 1$ y el resultado es obvio.

Supongamos ahora que el resultado es cierto para todo natural $k < n$. Ordenando la factorización de $X^n - 1$ dada en (3), tenemos que

$$X^n - 1 = \Phi_n(X). \prod_{d|n,1\le d<n} \Phi_d(X).$$

Por hipótesis inductiva, cada polinomio $\Phi_d(X)$ en la productoria tiene coeficientes enteros y, por definición, cada uno de estos polinomios es mónico. Luego, $\Phi_n(X)$ es el cociente entre $X^n - 1$ y este producto, que es un polinomio mónico a coeficientes enteros. Esto asegura que $\Phi_n(X)$ tiene todos sus coeficientes enteros. □

En lo que sigue, notaremos $\Gamma_n(X) := \prod_{d|n, 1\leq d<n} \Phi_d(X)$. Observemos que $X^d - 1$ divide a $\Gamma_n(X)$ para cualquier d divisor propio de n ya que todas las raíces de $X^d - 1$ son simples y son raíces también de $\Gamma_n(X)$. Más aún, como $X^d - 1$ es un polinomio mónico, el cociente resulta también un polinomio a coeficientes enteros.

Una última propiedad que vamos a usar de los polinomios ciclotómicos es la siguiente:

Lema 3.3 *Sea $n \in \mathbb{N}$. El polinomio $\Phi_n(X)$ es estrictamente creciente en $[1, +\infty)$. Si además, $n > 1$, $\Phi_n(2) \geq 2$.*

Demostración. Si $n = 1$ o $n = 2$, el enunciado es evidente, ya que $\Phi_1(X) = X - 1$ y $\Phi_2(X) = X + 1$. Si $n \geq 3$, todas las raíces de Φ_n son complejas no reales de módulo 1. Por lo tanto, Φ_n es producto de cuadráticas del tipo $(X - \xi).(X - \bar{\xi}) = X^2 - 2\cos\theta X + 1$ que no tienen raíces reales, y por lo tanto son siempre positivas y estrictamente crecientes en $[\cos\theta, +\infty)$. Luego Φ_n debe ser positiva y estrictamente creciente en $[1, +\infty)$. Entonces, teniendo en cuenta que $\Phi_n(X)$ tiene todos sus coeficientes enteros, $\Phi_n(2) > \Phi_n(1) \geq 1$ y por lo tanto, $\Phi_n(2) \geq 2$. □

4 El resultado principal

Siguiendo con las notaciones anteriores, dado $n \in \mathbb{N}$ tenemos dos polinomios $\Phi_n(X)$ y $\Gamma_n(X)$ con coeficientes enteros que son coprimos. Aplicando el algoritmo de Euclides en $\mathbb{Q}[X]$ obtenemos que existen polinomios $r_n(X), s_n(X) \in \mathbb{Q}[X]$ tales que

$$1 = r_n(x).\Phi_n(X) + s_n(X).\Gamma_n(X).$$

Sea $\ell_n \in \mathbb{N}$ el mínimo común múltiplo entre todos los denominadores de los coeficientes de $r_n(X)$ y $s_n(X)$. Multiplicando la igualdad anterior por ℓ_n obtenemos polinomios $R_n(X), S_n(X)$ *con coeficientes enteros* tales que

$$\ell_n = R_n(x).\Phi_n(X) + S_n(X).\Gamma_n(X). \tag{4}$$

Ahora tenemos todos los ingredientes como para demostrar nuestro resultado principal:

Teorema 4.1 *Dado $n \in \mathbb{N}$, existen infinitos primos de la forma $p = q.n + 1$, con $q \in \mathbb{N}$.*

Demostración. Evaluemos la identidad (4) en $2.\ell_n$:

$$\ell_n = P_n(2.\ell_n).\Phi_n(2.\ell_n) + R_n(2.\ell_n).\Gamma_n(2.\ell_n).$$

Como todos los polinomios involucrados tienen coeficientes enteros, ésta igualdad vale en $\mathbb{Z}$. Sea p un primo que divide a $\Phi_n(2.\ell_n) \geq 2$. Entonces p divide a $\Phi_n(2.\ell_n).\Gamma_n(2.\ell_n) = (2\ell_n)^n - 1$ y, por lo tanto, p es coprimo con $2.\ell_n$. Entonces, p no puede dividir a $\Gamma_n(2.\ell_n)$, de lo contrario p dividiría a ℓ_n. Como para todo d divisor positivo de n tal que $d < n$, $\Gamma_n(X) = (X^d - 1).Q_d(X)$ para algún polinomio a coeficientes enteros $Q_d(X)$, resulta que p no puede dividir a $(2.\ell_n)^d - 1$ para ningún d, pues si no, dividiría a $\Gamma_n(2.\ell_n)$. Notar entonces que estamos en las condiciones del Lema 2.1: p divide a $(2\ell_n)^n - 1$ y no divide a $(2.\ell_n)^d - 1$ para todo d divisor positivo de n menor que n. Luego p es de la forma deseada, $p = q.n + 1$.

Hasta ahora, hemos obtenido solo un primo que cumple lo pedido. Para demostrar la infinitud, utilizamos a una idea similar a la de Euclides. Supongamos que hay finitos primos $p_1, \ldots, p_s$ congruentes a 1 módulo n. Si consideramos $\Phi_n(2.\ell_n.p_1 \ldots p_s) \geq 2$, y tomamos p primo positivo que lo divida, siguiendo la demostración anterior, p resulta congruente a 1 mod n. Sin embargo, como $p \mid \Phi_n(2.\ell_n.p_1.\ldots.p_s).\Gamma_n(2.\ell_n.p_1.\ldots.p_s) = (2\ell_n.p_1.\ldots.p_s)^n - 1$, p no puede ser ninguno de los p_i, lo que nos lleva a un absurdo que provino de suponer la finitud de estos primos. □

Observación 4.2 *Notar que, con las notaciones anteriores, dado cualquier número natural m, la demostración del teorema nos asegura que si p es un primo positivo, tal que $p \mid \Phi_n(m)$ y $(p, \ell_n) = 1$, entonces $p \equiv 1$ (mód n).*

En lo que sigue, vamos a ver cómo el teorema anterior nos permite calcular los primos buscados en un ejemplo.

Ejemplo 4.3

Sea $n = 12$. Calculemos primero los polinomios ciclotómicos involucrados:

$$\Phi_1(X) = X - 1; \quad \Phi_2(X) = \frac{X^2 - 1}{\Phi_1(X)} = X + 1; \quad \Phi_3(X) = \frac{X^3 - 1}{\Phi_1(X)} = X^2 + X + 1$$

$$\Phi_4(X) = \frac{X^4 - 1}{\Phi_1(X)\Phi_2(X)} = X^2 + 1; \quad \Phi_6(X) = \frac{X^6 - 1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)} = X^2 - X + 1$$

$$\Phi_{12}(X) = \frac{X^{12} - 1}{\Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_4(X)\Phi_6(X)} = X^4 - X^2 + 1.$$

Luego, los polinomios de la identidad (4) en nuestro caso serán:

$$\Phi_{12}(X) = X^4 - X^2 + 1 \quad \text{y} \quad \Gamma_{12}(X) = \frac{X^{12} - 1}{\Phi_{12}(X)} = X^8 + X^6 - X^2 - 1.$$

El algoritmo de Euclides para estos polinomios nos da

$$1 = (\frac{2}{3} + \frac{1}{2}X^2 - \frac{1}{6}X^6)(X^4 - X^2 + 1) + (-\frac{1}{3} + \frac{1}{6}X^2)(X^8 + X^6 - X^2 - 1).$$

Luego, la ecuación (4) en este caso queda

$$6 = (4 + 3X^2 - X^6)(X^4 - X^2 + 1) + (-2 + X^2)(X^8 + X^6 - X^2 - 1).$$

Para obtener el primer primo congruente a 1 módulo 12, evaluamos Φ_{12} en $2.6 = 12$ y da 20593 que es ya es primo. Para obtener el próximo, habría que evaluar Φ_{12} en $2.6.20593$ lo que da 3729095127575903994481 que es producto de los primos 349 y 10685086325432389669, ambos congruentes a 1 módulo 12.

Como puede verse, este procedimiento rápidamente da números grandes. Sin embargo, si usamos la Observación 4.2, evaluando el polinomio en cualquier número, y considerando todos los primos que aparecen en la factorización salvo eventualmente el 2 y el 3, obtenemos primos congruentes a 1 módulo 12 más chicos. Así, aparecen $\Phi_{12}(2) = 13$, $\Phi_{12}(3) = 73$, $\Phi_{12}(4) = 241$, $\Phi_{12}(5) = 601$, $\Phi_{12}(6) = 13.97$, $\Phi_{12}(7) = 13.181$, $\Phi_{12}(8) = 37.109$, $\Phi_{12}(9) = 6481$, $\Phi_{12}(10) = 9901$ y $\Phi_{12}(11) = 13.1117$. En el caso en particular del 12, 2 y 3 nunca van a aparecer en la factorización de $\Phi_{12}(m)$ ya que, para cualquier valor entero de m, $m^4 - m^2 + 1 \equiv 1$ (mód 6).

5 Algunos casos particulares

5.1 El caso n primo

Cuando $n > 2$ es primo, $\Phi_n(X) = \sum_{i=0}^{n-1} X^i$ y $\Gamma_n(X) = X - 1$. En este caso, podemos escribir explícitamente el algoritmo de Euclides de la identidad (4) entre estos polinomios:

$$n = 1.\Phi_n(X) - (\sum_{i=0}^{n-2}(n - 1 - i)X^i).\Gamma_n(X).$$

En particular, $\Phi_n(2) = 2^n - 1$ es coprimo con n (pues usando el pequeño teorema de Fermat, $2^n - 1 \equiv 1$ (mód n)). Luego, aplicando el Teorema 4.1, obtenemos una propiedad clásica de los números de Mersenne que dice que cualquier primo que divida a $2^n - 1$ debe ser congruente a 1 módulo n. También podemos deducir que existe un primo $p \equiv 1$ (mód n) con $p \leq 2^n - 1$.

5.2 El caso $n = 2^k$

Cuando $n = 2^k$ con $k \in \mathbb{N}$, $\Phi_n(X) = X^{2^{k-1}} + 1$ y $\Gamma_n(X) = X^{2^{k-1}} - 1$. En este caso, vale que

$$2 = 1.\Phi_n(X) - 1.\Gamma_n(X).$$

Por lo tanto, evaluando en 2, tenemos que cualquier primo que divida al número de Fermat $2^{2^{k-1}} + 1$ debe ser congruente a 1 módulo 2^k, y también tenemos una cota del estilo del caso anterior: existe un primo $p \equiv 1$ (mód n) con $p \leq 2^{\frac{n}{2}} - 1$.

Referencias

[1] G. L. Dirichlet. *Dirichlet's Werke.* Berlin, 1889.

[2] T. Estermann. Note on a paper of A. Rotkiewicz. *Acta Arith.*, 8:465–467, 1963.

[3] G. Hardy and E. Wright. *An introduction to the theory of numbers.* Oxford, 1960.

[4] T. Nagell. *Introduction to number theory.* Wiley, New York, 1951.

[5] I. Niven and B. Powell. Primes in certain arithmetic progressions. *Am. Math. Mon.*, 83:467–469, 1976.

[6] A. Rotkiewicz. Démonstration arithmétique de l'existence d'une infinité de nombres premiers de la forme $nk + 1$. *Enseign. Math.,* (2) 7:277–280, 1962.

[7] A. Selberg. An elementary proof of Dirichlet's theorem about primes in an arithmetic progression. *Ann. Math.*, (2) 50:297–304, 1949.

[8] W. Sierpinski. *Elementary theory of numbers.* Hafner, New York, 1964.

[9] E. Wendt. Elementarer Beweis des Satzes, dass in jeder unbegrenzten arithmetischen Progression $my+1$ unendlich viele Primzahlen vorkommen. *J. für Math.* CXV. 85-88, 1895.

[10] H. Zassenhaus. Über die Existenz von Primzahlen in arithmetischen Progressionen. *Comment. Math. Helv.*, 22:232–259, 1949.

Departamento de Matemática, FCEyN - Departamento de Cs. Exactas, CBC.
Universidad de Buenos Aires - Ciudad Universitaria - Pabellón I 1428 - Buenos Aires - Argentina.