Miscelánea Matemática **50** (2009) 57–76 SMM

Postulado de Bertrand y distribución de los números primos[1]

Gabriel Villa Salvador
Departamento de Control Automático
Centro de Investigación y de Estudios Avanzados del I.P.N.
y
Departamento de Matemáticas
Universidad Autónoma Metropolitana Iztapalapa
gvilla@ctrl.cinvestav.mx, gvs@xanum.uam.mx

Resumen

El énfasis principal en este trabajo será lo que se conoce como *"el postulado de Bertrand"* el cual establece que para cualquier número natural n, entre n y $2\,n$ existe al menos un número primo.

También hablaremos de algunas propiedades de los números primos en general. Por ejemplo veremos que para cualesquiera dos números naturales k y n existen n enteros consecutivos que son divididos por al menos k números primos distintos y abordaremos varios problemas en la teoría clásica de números. Algunos de ellos son relativamente fáciles de enunciar, pero son extremadamente difíciles de demostrar. Por ejemplo el famosísimo "Último Teorema de Fermat" planteado por Pierre de Fermat, posiblemente en 1637, y resuelto completamente por Andrew Wiles entre los años 1993 y 1995, es decir, aproximadamente 358 años después.

[1]Este artículo está basado en la conferencia del mismo nombre presentada el 27 de octubre de 2005 en el XXXVIII Congreso de la Sociedad Matemática Mexicana en la Escuela Superior de Física y Matemáticas del Instituto Politécnico Nacional.

Discutiremos los siguientes problemas:

(1) Último Teorema de Fermat.

(2) Dado un $n \in \mathbb{N}$, ¿que números primos p se pueden escribir de la forma $p = x^2 + ny^2, x, y \in \mathbb{Z}$?

(3) Dado un número real x, ¿cuántos primos hay entre 1 y x?

(4) Dados $a, b \in \mathbb{Z}$ primos relativos, ¿cuántos primos de la forma $p = a + nb$ existen?

1. Último Teorema de Fermat

La siguiente es una breve síntesis de la historia del Último Teorema de Fermat (UTF).

Al margen de su libro "Arithmetica" de Diofanto, después del problema VIII del Libro 2 donde Diofanto resuelve un caso particular de escribir un cuadrado como la suma de dos cuadrados, Pierre de Fermat (1601-1665) escribió (se cree que en 1637):

"*Es imposible separar un cubo en dos cubos o un bicuadrado en dos bicuadrados o en general cualquier potencia mayor que la segunda en dos potencias similares; he descubierto una prueba realmente maravillosa que no puede ser escrita en el margen de este libro por ser éste demasiado pequeño*".

En otras palabras, Fermat afirmó:

Teorema 1.1 (Fermat ¿1637?) *Para $n > 2$, no existen $x, y, z \in \mathbb{N}$ tales que $x^n + y^n = z^n$.* ❀

Algunos resultados parciales de este teorema no son difíciles de demostrar. Por ejemplo sean $x, y \in \mathbb{N}$ con $y \geq x$ fijos, $n \in \mathbb{N}$ y sea $z_n = (x^n + y^n)^{1/n}$. Entonces z_n es decreciente y $\lim_{n\to\infty} z_n = y$, por lo que existe $n_0 \in \mathbb{N}$ tal que para toda $n \geq n_0$, $z_n < y + 1$. Por otro lado, $z_n > y$ para toda $n \geq 1$, es decir $y < z_n < y + 1$ para $n \geq n_0$. Esto implica que $z_n \notin \mathbb{Z}$ para toda $n \geq n_0$. Esto prueba el siguiente

Teorema 1.2 *Para $x, y \in \mathbb{N}$, existe n_0 tal que para toda $n \geq n_0$ la ecuación $x^n + y^n = z^n$ no tiene solución $z \in \mathbb{Z}$.* ❀

La historia está llena de falsas demostraciones del UTF. Los intentos para demostrar el UTF han dado lugar a innumerables teorías, por ejemplo, la Teoría de los Campos Ciclotómicos, los grupos de clases, diversos temas en la Geometría Algebraica, el desarrollo vigoroso de la teoría de congruencias inventada por F. Gauss [12], primos regulares y primos irregulares, Dominios de Factorización Única, la Teoría de Ideales de Kummer, los Dominios de Dedekind, la Teoría de Campos de Clase, etc. Aquí mencionamos uno de estos intentos fallidos.

El primero de marzo de 1847 Gabriel Lamé en Paris anunció una demostración del UTF, la cual nunca publicó y que el creía que era similar a su prueba del Teorema 1.1 para el caso especial de $n = 7$. Su argumento se basa en lo siguiente: sea p un número primo y sea

$$x^p + y^p = \prod_{i=0}^{p-1} \left(x + \zeta_p^i y\right) = z^p, \text{ donde } \zeta_n = e^{(2\pi i/n)}, n \in \mathbb{N}.$$

Al tomar ideales en $\mathbb{Z}[\zeta_p] \subseteq \mathbb{Q}(\zeta_p)$, el cual se llama *campo ciclotómico de las p–raíces de la unidad*, demostró que $\left(x + \zeta_p^i y\right) = A_i^p$ y concluyó que $A_i = (\alpha_i)$ por ser $x + \zeta_p^i y$ y $x + \zeta_p^j y$ primos relativos para $i \neq j$ en $\mathbb{Z}[\zeta_p]$. De aquí se deriva una contradicción.

Lo importante para nosotros en este contexto es la introducción de la n-ésima raíz primitiva de la unidad, $\zeta = \zeta_n = e^{(2\pi i/n)}$. El error fundamental en la demostración de Lamé, primero cuestionado por Liouville, el cual recibió una carta de Ernst Edward Kummer que, basado en la evidencia que se infería de lo comunicado por Lamé, refutaba la base de la demostración, y que fue tratado de remediar por Cauchy pero que fue finalmente desmentido por el mismo Kummer, fue el de suponer que si $A^p = (\beta)$ es principal, entonces A es principal. Lo anterior fue supuesto por Lamé pues él creyó que el anillo de enteros $\mathbb{Z}[\zeta_p]$ era de ideales principales, es decir, que el número de clase del campo ciclotómico era uno (de hecho, sólo se necesita, para la validez de la afirmación, que p no divida al número de clase del campo ciclotómico $\mathbb{Q}(\zeta_p)$. Sin embargo, también esto último es falso). Más aún, se tiene que el campo ciclotómico $\mathbb{Q}(\zeta_m), m \not\equiv 2 \text{ mód } 4$, tiene número de clase igual a uno si y sólo si m es uno del los siguientes números:

$$1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33,$$
$$35, 36, 40, 44, 45, 48, 60, 84$$

los cuales son únicamente 30 casos.

Ahora bien, sea $K = \mathbb{Q}\left(\sqrt{D}\right)$, con $D < 0$ y libre de cuadrados, entonces el número de clase de K es uno si y sólo si $D = 1, 2, 3, 7, 11, 19, 43,$

67, 163. El problema de determinar los campos cuadráticos con número de clase uno fue terminado hasta 1967 por Stark.

Volviendo al UTF, se fueron probando algunos casos:

1640:	$n = 3$(¿?), $n = 4$	Fermat
1753:	$n = 3$	Euler
1825 ó 1828:	$n = 5$	Dirichlet, Legendre
1839:	$n = 7$	Lamé
1847:	n regular	Kummer
1930:	$n < 600$	Vandiver
1951:	$n < 4000$	Lehmer
1977:	$n < 125,000$	Wagstaff
1992:	$n < 4,000,000$	Buhler y otros
1993-1995:	$n \geq 3$	Wiles

Al estudiar curvas más generales, Mordell conjeturó [17]:

Conjetura 1.3 (Conjetura de Mordell (1922)) *Si una curva $F(x, y, z)$ en $\mathbb{Z}$ tiene género $g \geq 2$, el número de soluciones en $\mathbb{Q}$ es esencialmente finito.*

Por esencialmente finito queremos decir que las soluciones (x_0, y_0, z_0) y $(\lambda x_0, \lambda y_0, \lambda z_0)$ con $\lambda \neq 0$, las consideramos equivalentes y que sólo hay un número finito de soluciones inequivalentes a pares.

Faltings probó en 1983 la conjetura de Mordell. Este es el resultado que antes del probado por Wiles se acercó más a la solución final del UTF.

Teorema 1.4 (Faltings 1983 [9]) *Para $n \geq 3$, el número de soluciones x, y, z de la ecuación $x^n + y^n = z^n$, $x, y, z \in \mathbb{N}, x, y, z$, primos relativos, es esencialmente finita.* ❀

Para finalizar, la última parte de la historia de la demostración del UTF, es la siguiente:

Una curva elíptica es una curva del tipo $y^2 = f(x)$ con

$$f(x) = x(x - A)(x - B), \quad A, B \in \mathbb{Z} \setminus \{0\}, \quad A \neq B.$$

En lugar de preguntarnos que tan a menudo se tiene $y^2 = f(x)$ nos preguntamos que tan a menudo tenemos $y^2 \equiv f(x)$ mód p donde p un número primo arbitrario.

Para cada número primo p , sea N_p el número de pares de enteros (x, y) que satisfacen: $0 \leq x, y \leq p - 1$ y $y^2 - f(x) \equiv 0$ mód p.

En 1814, Gauss encontró una forma para calcular N_p para la curva

$$y^2 = x^3 - x.$$

$N_2 = 2$
De hecho: $N_p = p$ si $p \equiv 3$ mód 4
$N_p =$ más complicada si $p \equiv 1$ mód 4.

Una curva elíptica se llama *modular* si $N_2, N_3, N_5, \ldots$ satisfacen alguna regla que nos dé una estructura similar a la fórmula de Gauss. Esta sucesión debe ser muy especial para tener esta propiedad modular.

Conjetura 1.5 (Taniyama 1955 y Shimura 1962 [21]) *Se tiene que toda curva elíptica es modular.*

Teorema 1.6 (Gerhard Frey (1985) [10]) *Supongamos que existe un contraejemplo al UTF: $a^n + b^n = c^n$ con $n > 2$, $a, b, c \in \mathbb{N}$. Consideremos entonces la curva elíptica $y^2 = x(x - a^n)(x + b^n)$. Esta curva "parece" ser no modular.* ❀

Teorema 1.7 (Ribet (1986) [18]) *La curva de Frey es no modular.* ❀

Teorema 1.8 (Wiles (1993-1995) [25, 22]) *La curva de Frey es modular.* ❀

Conclusión 1.9 *No hay contraejemplos al Último Teorema de Fermat, por lo cual éste es cierto.*

2. Primos de la forma $p = x^2 + ny^2$

En esta sección queremos determinar qué números primos son de la forma $x^2 + ny^2$ con $x, y \in \mathbb{N}$ fijos. Notemos que x y y deben ser primos relativos pues si $p = x^2 + ny^2$ y $d|x$ y $d|y$, entonces $d^2|p$.

Consideremos ahora esta pregunta para el caso particular $n = 1$. Es decir, ¿que primos p son tales que $p = x^2 + y^2$? En un curso de teoría de anillos de la licenciatura se prueba que $p = x^2 + y^2 \iff p = 2$ $(2 = 1^2 + 1^2)$ ó $p \equiv 1$ mód 4.

La idea básica es considerar el anillo de los enteros gaussianos $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$ donde $i = \sqrt{-1}$ y probar que $p \equiv 1$ mód 4 no es primo en $\mathbb{Q}(i)$ sino que $p = (a + bi)(a - bi)$ en $\mathbb{Z}[i]$.

Además $(a+bi)$ y $(a-bi)$ son ideales primos en $\mathbb{Z}[i]$. Por otro lado $p \equiv 3$ mód 4 permanece primo en $\mathbb{Z}[i]$. En otras palabras, tenemos: si $p > 2$ es primo en $\mathbb{Q}$, entonces

$$(p) = \begin{cases} \wp_1\wp_2, & \text{si} \quad p \equiv 1 \text{ mód } 4, \\ \wp, & \text{si} \quad p \equiv 3 \text{ mód } 4, \end{cases}$$

con $\wp_1, \wp_2, \wp$ ideales primos de $\mathbb{Z}[i]$.

Ahora sea p un primo y sea $a \in \mathbb{Z}$. Entonces definimos el *símbolo de Legendre* por:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si} \quad p|a, \\ 1, & \text{si} \quad p \nmid a \text{ y } a \equiv x^2 \text{ mód } p, \text{ para alguna } x \in \mathbb{Z}, \\ -1, & \text{si} \quad p \nmid a \text{ y } a \not\equiv x^2 \text{ mód } p, \text{ para toda } x \in \mathbb{Z}. \end{cases}$$

Notemos que $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ mód p. La razón de esto es que si $\mathbb{F}_q$ denota el campo finito de q elementos, entonces $\mathbb{F}_q = \{x | x^q = x\} = \{x | x^{q-1} = 1\} \cup \{0\}$. Si $p|a$, entonces $\bar{a} := a$ mód $p = 0$ y el resultado es inmediato. Así se tiene que para $a \not\equiv 0$ mód p,

$$\mathbb{F}_p\left[\sqrt{\bar{a}}\right] = \begin{cases} \mathbb{F}_{p^2}, & \text{si} \quad \sqrt{\bar{a}} \notin \mathbb{F}_p \quad (\iff \left(\frac{a}{p}\right) = -1), \\ \mathbb{F}_p, & \text{si} \quad \sqrt{\bar{a}} \in \mathbb{F}_p \quad (\iff \left(\frac{a}{p}\right) = 1). \end{cases}$$

Si $\bar{b} = \sqrt{\bar{a}}$, $\bar{b}^2 = \bar{a}$, $\bar{a}^{p-1} = 1 \Longrightarrow a^{\frac{p-1}{2}} = b^{p-1} = \pm 1$ mód p. Se sigue que $a^{\frac{p-1}{2}} = 1 \iff b^{p-1} = 1 \iff \bar{b} \in \mathbb{F}_p \iff \sqrt{\bar{a}} \in \mathbb{F}_p \iff \left(\frac{a}{p}\right) = 1$.

En particular $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \iff p \equiv 1 \text{ mód } 4, \\ -1 & \iff p \not\equiv 1 \text{ mód } 4 \\ & \quad (\iff p \equiv 3 \text{ mód } 4). \end{cases}$

Por lo tanto $p = x^2 + y^2 \iff \left(\frac{-1}{p}\right) = 1$.

En general se tiene

Teorema 2.1 (Ley de Reciprocidad Cuadrática [12]) *Si p, q son primos impares, entonces* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$. ❀

Una demostración de la ley de reciprocidad se puede dar usando la descomposición de primos en campos ciclotómicos [23].

Regresando a nuestro problema, tenemos: $p|x^2+ny^2$ con $(x,y)=1 \iff \left(\frac{-n}{p}\right)=1$. De hecho tenemos, $p|x^2+ny^2 \iff x^2+ny^2 \equiv 0 \text{ mód } p$ y puesto que $(x,y)=1$, entonces $(p,y)=1$. Por lo tanto y tiene inverso en $\mathbb{F}_p$, es decir, existe z tal que $yz \equiv 1 \text{ mód } p$ y esto implica que $(xz)^2+n \equiv 0 \text{ mód } p$, por lo que $n \equiv -(xz)^2 \text{ mód } p$ es equivalente a $\left(\frac{-n}{p}\right)=1$.

Veamos ahora el caso $n=3$. Usando la ley de reciprocidad cuadrática, se tiene que

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{(p-1)(3-1)}{2}}=$$
$$(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)=(-1)^{p-1}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right)=$$
$$\begin{cases} 1, & \text{si} \quad p \equiv 1 \text{ mód } 3, \\ -1, & \text{si} \quad p \equiv -1 \text{ mód } 3, \end{cases}$$

Entonces se sigue que $p=x^2+3y^2, x, y \in \mathbb{Z} \iff p=3$ $(x=0, y=1)$ ó $p \equiv 1 \text{ mód } 3$. Por supuesto necesitamos hacer algo más que lo establecido en el párrafo anterior para probar que $p=x^2+3y^2$ con $x, y \in \mathbb{Z}$ si p es un número primo tal que $p \equiv 1 \text{ mód } 3$.

Por ejemplo tenemos $13=1^2+3\cdot 2^2$ y $31=2^2+3\cdot 3^2$.

Si $n=2$, $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}}$, por tanto $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ $=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}=1 \iff (-1)^{\frac{p-1}{2}}=(-1)^{\frac{p^2-1}{8}}=\left((-1)^{\frac{p-1}{2}}\right)^{\frac{p+1}{4}}$ lo cual es equivalente a $(-1)^{\frac{p-1}{2}}=1$ ó $(-1)^{\frac{p-1}{2}}=1$ y $\frac{p+1}{4} \equiv 1 \text{ mód } 2 \iff p \equiv 1 \text{ mód } 4$ ó $p \equiv 3 \text{ mód } 4$ y $p \equiv 3 \text{ mód } 8 \iff p \equiv 1,3,5 \text{ mód } 8$.

Ahora $p=x^2+2y^2$ es imposible con $p \equiv 5 \text{ mód } 8$ lo cual es fácil de verificar viendo las posibilidades x, y par, o impar. De hecho, si x es par, x^2+2y^2 es par; si x es impar y y es impar, $x^2+2y^2 \equiv 1 \text{ mód } 8$ y finalmente si x es impar y y es par, $x^2+2y^2 \equiv 3 \text{ mód } 8$.

Así pues tenemos que si $p=x^2+2y^2$, entonces $p \equiv 1,3 \text{ mód } 8$. El recíproco también es cierto.

En general se tiene

Teorema 2.2 ([1], Theorem 9.2) *Sea $n \in \mathbb{N}$. Entonces existe un polinomio mónico irreducible $f_n(x) \in \mathbb{Z}[x]$ tal que si un primo impar*

no divide a n ni al discriminante de $f_n(x)$, entonces

$$p = x^2 + ny^2 \iff \left(\frac{-n}{p}\right) = 1 \text{ y}$$
$$f_n(x) \equiv 0 \text{ mód } p \text{ tiene solución entera.} \qquad \text{❀}$$

Ejemplo 2.3 *Para $n = 27$ se tiene $f_{27}(x) = x^3 - 2$. Para $n = 64$, $f_{64}(x) = x^4 - 2$. Para $n = 14$, $f_{14}(x) = (x^2 + 1)^2 - 8$.*

Observación 2.4 *Se tiene que el grado del polinomio $f_n(x)$ del Teorema 2.2 es $h(-4n)$ donde $h(D)$ es el número de clases de formas cuadráticas primitivas positivas de discriminante D y es igual al número de clases de formas cuadráticas reducidas de discriminante D.*

Con el fin de aclarar la terminología de la Observación 2.4, a continuación damos algunas definiciones y propiedades de las formas cuadráticas.

Una forma cuadrática es de la forma: $g(x, y) = ax^2 + bxy + cy^2$ con $a, b, c \in \mathbb{Z}$ y el *discriminante* de $g(x, y)$ se define por $D = b^2 - 4ac$.

Dos formas $f(x, y)$ y $g(x, y)$ se llaman *equivalentes* si existen p, q, r, $s \in \mathbb{Z}$ tales que $ps - qr = \pm 1$ y

$$f(x, y) = g(px + qy, rx + sy).$$

Si $ps - qr = 1$ la equivalencia se llama *propia* y se llama *impropia* si $ps - qr = -1$. Dos formas equivalentes tienen el mismo discriminante.

Una forma $g(x, y) = ax^2 + bxy + cy^2$ se llama *primitiva* si a, b y c son primos relativos.

Si $g(x, y) = ax^2 + bxy + cy^2$, entonces

$$4ag(x, y) = (2ax + by)^2 - Dy^2.$$

Por lo que si $D > 0$, entonces $g(x, y)$ representa tanto enteros positivos como negativos. Si $D < 0$, entonces $g(x, y)$ sólo representa enteros positivos o sólo enteros negativos dependiedo si $a > 0$ o $a < 0$. Una forma cuadrática $g(x, y)$ se llama *positiva definida* si $g(x, y) > 0$ para todo $x, y \in \mathbb{Z}$ con $(x, y) \neq (0, 0)$.

Una forma primitiva positiva $ax^2 + bxy + cy^2$ se llama *reducida* si

$$|b| \leq a < c \text{ y } b \geq 0 \text{ ya sea que } |b| = a \text{ o } a = c.$$

Como una última observación, mencionamos que se tiene que $h(-4n) = 1$ si y sólo si $n = 1, 2, 3, 4$ o 7 [1, Theorem 2.18].

3. Distribución de los números primos y el Teorema de Dirichlet

Teorema 3.1 (Euclides, 300 A.C.) *Sea $x \in \mathbb{R}, x > 0$ y sea*

$$\pi(x) = \big|\{p|p \text{ es un número primo}, 2 \leq p \leq x\}\big|.$$

Entonces:

$$\lim_{x\to\infty} \pi(x) = \infty.$$

Demostración: Daremos tres demostraciones con el fin de obtener más información de la función $\pi(x)$.

1.ª Demostración: (Euclides) [7, Proposition 20]

Sea $A = \{p|p \geq 2, p \text{ número primo}\}$ y supongamos que $|A| = m < \infty$, consideremos $t = \left(\prod_{p\in A} p\right) + 1$. Puesto que todo número es producto de primos, existe $q \in A$, tal que $q|t$, por lo que $q|t - \left(\prod_{p\in A} p\right) = 1$ lo que es una contradicción. ❀

2.ª Demostración:

Supongamos que $A = \{p_1, \ldots, p_m\}$. Sea $x > 0$, $x \in \mathbb{R}$, $n \in \mathbb{N}$, $2 \leq n \leq x$. Entonces existen $\alpha_1, \ldots, \alpha_m \in \mathbb{N} \cup \{0\}$ tales que $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m} \leq x$, por lo que $\sum_{i=1}^{m} \alpha_i \log p_i \leq \log x$, por lo tanto $\alpha_i \leq \frac{\log x}{\log p_i} \leq \frac{\log x}{\log 2}$, $i = 1, \ldots, m$. Esto nos dice que tenemos a lo más $\frac{\log x}{\log 2} + 1$ posibles exponentes , es decir tenemos a lo más $\left(\frac{\log x}{\log 2} + 1\right)^m$ posibles enteros $n \in [2, x]$, es decir $x - 1 \leq \left(\frac{\log x}{\log 2} + 1\right)^m$, lo cual contradice que $\lim_{x\to\infty} \frac{x}{(\log x)^m} = \infty$ para cualquier m. ❀

3.ª Demostración: (Euler) [8]

Otra vez supongamos que $A = \{p_1, \ldots, p_m\}$ es finito. Entonces dado $n \in \mathbb{N}$, $n = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$, $\alpha_i \in \mathbb{N} \cup \{0\}$, entonces $\sum_{n=1}^{\infty} \frac{1}{n} =$

$$\sum_{\alpha_1,\ldots,\alpha_m=0}^{\infty} \frac{1}{p_1^{\alpha_1}\cdots p_m^{\alpha_m}} = \prod_{i=1}^{m}\left(\sum_{k=0}^{\infty}\frac{1}{p_i^k}\right) = \prod_{i=1}^{m}\frac{1}{1-\frac{1}{p_i}} = \prod_{i=1}^{m}\frac{p_i}{p_i-1} < \infty,$$

lo cual es absurdo. ❀

Ahora analicemos las demostraciones anteriores para obtener información acerca de $\pi(x)$. De la demostración de Euclides, enumeremos todos los números primos: $2 = p_1 < p_2 < \ldots$. Dado m, existe p_k, $k \geq m+1$ tal que $p_k | (p_1 \cdots p_m + 1)$, por lo que $p_{m+1} \leq p_1 \cdots p_m + 1$. De aquí se sigue que $p_{m+1} \leq 2^{2^{m+1}} + 1$, por lo que $p_n \leq 2^{2^n}$ para toda n. Se sigue que $\log_2(\log_2(p_n)) \leq n$.

Ahora si $2^{2^n} \leq x < 2^{2^{n+1}}$, $\pi(x) \geq \pi\left(2^{2^n}\right) \geq \pi(p_n) = n$. Finalmente obtenemos:

$$\pi(x) \geq n \geq \log_2(\log_2(x)).$$

De la segunda prueba, se tiene que si $p_1 \ldots p_m$ son todos lo primos $\leq x$, $m = \pi(x)$ y $x - 1 \leq \left(\frac{\log x}{\log 2} + 1\right)^m$ por lo que

$$\pi(x) \geq \frac{\log(x-1)}{\log\left(\frac{\log x}{\log 2} + 1\right)}.$$

Utilizando algunas de estas ideas, Gauss y Legendre conjeturaron (conjetura probada al final del siglo XIX por Hadamard y Vallée de Poussin independientemente):

Teorema 3.2 (Teorema de los Números Primos [14, 2, 20])

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1.$$ ❀

Las ideas de la demostración están basadas en la demostración de Dirichlet del siguiente resultado:

Teorema 3.3 (Dirichlet, 1839-1840 [3, 19]) *Si $a, b \in \mathbb{N}$ con $(a, b) = 1$, entonces si $\mathcal{A} = \{p | p$ primo y $p \equiv a$ mód $b\}$, se tiene $\sum_{p\in A} \frac{1}{p} = \infty$. En particular $\mathcal{A}$ es infinito.* ❀

Una parte crucial de la demostración del teorema anterior consiste en usar las series L de Dirichlet: $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$, $\mathbb{R}e\ s>1$, donde $\chi:\mathbb{Z}\longrightarrow\mathbb{C}^*$ es tal que ó $\chi\equiv 1$ ó χ satisface $\chi(a+f)=\chi(a)$ para algún f; $\chi(a)=0$ si $(a,f)\neq 1$; $\chi(ab)=\chi(a)\chi(b)$. La parte fundamental es probar que $L(1,\chi)\neq 0$ donde χ es un caracter real diferente al principal, es decir $\chi\neq 1$.

Dado lo anterior, entonces se prueba que si $\mathcal{A}=\{p|p$ es primo y $p\equiv a$ mód $b\}$, entonces $\sum_{p\in\mathcal{A}}\frac{1}{p}=\infty$. En particular $\mathcal{A}$ es infinito.

El teorema de Dirichlet, nos contesta la pregunta: dados $a,b\in\mathbb{Z}$, ¿cuántos primos p hay de la forma $p\equiv a$ mód b?, notemos que si a y b no son primos relativos, digamos $d=(a,b)$, entonces si $p\equiv a$ mód b, entonces $p=a+sb, d|a, d|b\Longrightarrow d|p$ por lo que hay a lo más un primo con esta propiedad.

Podemos dar una demostración a un caso particular al teorema de Dirichlet. Por ejemplo, cuando $a=1$ y $b=n$ es arbitrario usando polinomios ciclotómicos (a continuación damos un esquema de demostración). También podemos probar directamente el caso $a=3, b=4$.

Se define, para $n\in\mathbb{N}$, el *n-ésimo polinomio ciclotómico* por

$$\Phi_n(x)=\prod_{\substack{j=0\\(j,n)=1}}^{n-1}\left(x-\zeta_n^j\right).$$

Se sabe que $\Phi_n(x)\in\mathbb{Z}[x]$ y es irreducible, $\mathbb{Q}(\zeta_n)\cong\mathbb{Q}[x]/\langle\Phi_n(x)\rangle$. El grado de $\Phi_n(x)$ es $\varphi(n)=|\{j\in\mathbb{N}|j\leq n,(j,n)=1\}|$.

Además, por inducción se tiene $x^n-1=\prod_{d|n}\Phi_d(x)$ y por la fórmula de inversión de Möbius se tendrá que $\Phi_n(x)=\prod_{d|n}\left(x^d-1\right)^{\mu\left(\frac{n}{d}\right)}$, donde

$$\mu(n)=\begin{cases}1, & \text{si } n=1,\\ (-1)^r, & \text{si } n=p_1\cdots p_r, p_1,\cdots,p_r \text{ primos distintos},\\ 0, & \text{si existe un número primo } p \text{ tal que } p^2|n.\end{cases}$$

Se tiene que $\Phi_1(x)=x-1, \Phi_2(x)=x+1, \Phi_3(x)=x^2+x+1, \Phi_4(x)=x^2+1, \Phi_5(x)=x^5+x^4+x^3+x^2+x+1, \Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+\cdots+x+1$, p un número primo.

Consideremos $p\nmid n$, p primo, y sea $a\in\mathbb{Z}$. Entonces $o(a \text{ mód } p)=n\Longleftrightarrow p|\Phi_n(a)$ ($o(a \text{ mód } p)=n$ significa que $a^n\equiv 1$ mód p y que para toda $0<m<n$, se tiene $a^m\not\equiv 1$ mód p).

En efecto, si $p|\Phi_n(a), x^n - 1 = \prod_{d|n} \Phi_d(x), a^n - 1 = \prod_{d|n} \Phi_d(a) \equiv 0 \text{ mód } p$ pues $p|\Phi_n(a)$. Por lo tanto $a^n \equiv 1 \text{ mód } p$. Si $m < n$ y si $o\,(a \text{ mód } p) = m$, entonces $a^m - 1 = \prod_{d|m} \Phi_d(a) \equiv 0 \text{ mód } p$, por lo tanto $p|\Phi_d(a), d \leq m < n$, pero puesto que Φ_d, Φ_n son irreducibles distintos, existen $\alpha(x), \beta(x) \in \mathbb{Z}[x]$ tales que $1 = \alpha(x)\Phi_d(x) + \beta(x)\Phi_n(x)$ lo cual implica que $p|1 = \alpha(a)\Phi_d(a) + \beta(a)\Phi_n(a)$ lo cual es absurdo.

Recíprocamente, si $o\,(a \text{ mód } p) = n, p|a^n - 1$, por tanto $p|\Phi_d(a)$ para algún $d|n$. Si $d < n, a^d - 1 = \prod_{t|d} \Phi_t(a) \equiv 0 \text{ mód } p$ lo cual es absurdo.

Como consecuencia tenemos que: $p|\Phi_n(a)$ para algún $a \in \mathbb{Z} \iff p \equiv 1 \text{ mód } n$.

En efecto, si $p|\Phi_n(a)$ se tiene que a mód p tiene orden n. Ahora bien, el grupo de unidades de los enteros módulo p tiene orden $p - 1$, por lo que $n|p - 1$.

Recíprocamente, si $n|p-1$, el grupo de unidades de los enteros módulo p, U_p es cíclico, por lo que existe un elemento a tal que $o\,(a \text{ mód } p) = n$, por lo que $p|\Phi_n(a)$.

Con esto tenemos [23]:

Corolario 3.4 (caso especial del Teorema de Dirichlet) *Sea n un entero mayor o igual a 1. Entonces hay una infinidad de primos $p \equiv 1 \text{ mód } n$.*

DEMOSTRACIÓN: Supongamos que hay una cantidad finita de tales primos, digamos $p_1, \cdots, p_s$ son todos los de este estilo. Sea $m = np_1, \cdots p_s$ y sea $N \in \mathbb{Z}$. Entonces $\Phi_n(Nm) \underset{\substack{\uparrow \\ \text{por Möbius}}}{\equiv} \pm 1 \text{ mód } m$, por tanto $\Phi_n(Nm) \equiv \pm 1 \text{ mód } \begin{cases} n, \\ p_i, \end{cases}$ de donde $p_i \nmid \Phi_n(Nm)$. Para N suficientemente grande, $\Phi_n(Nm) \neq \pm 1$ puesto que $\Phi_n(Nm) \underset{N \to \infty}{\longrightarrow} \infty$. por lo que existe $p \notin \{p_1, \cdots, p_s\}, p \nmid n$, tal que $p|\Phi_n(Nm)$. Por tanto $p \equiv 1 \text{ mód } n$. ❀

Por ejemplo la demostración original de Euclides usa el caso $n = 2$, es decir, el polinomio $\Phi_2(x) = x + 1$, para probar que hay una infinidad de números primos. Para $n = 4$, se usa $\Phi_4(x) = x^2 + 1$ para dar una demostración, ampliamente conocida, de que hay una infinidad de primos de la forma $4n + 1$.

Ejercicio 3.5 *Probar directamente que hay una infinidad de primos de la forma* $8n+1$ *usando* $\Phi_8(x) = \dfrac{x^8-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} = \dfrac{x^8-1}{(x-1)(x+1)\,(x^2+1)} = \dfrac{x^8-1}{x^4-1} = x^4+1.$

4. Enteros consecutivos sin números primos

Por un lado tenemos, por el Teorema 3.2, que hay una infinidad de primos en cualquier sucesión artimética. Por otro lado probaremos a continuación que en los números enteros hay cualquier cantidad de enteros consecutivos todos ellos altamente divisibles y en particular no primos.

Teorema 4.1 *Para cualesquiera* $n,\ k \in \mathbb{N}$*, existen* n *enteros consecutivos tales que cada uno de ellos es divisible por al menos* k *primos distintos. En particular, para toda* n *existen* n *enteros consecutivos compuestos.*

Demostración: Lo haremos por inducción en k con n arbitrario.

Si $k=1$, sea $m \geq 2$ cualquiera y sea $\{m, m+1, \ldots, m+n-1\}$ un conjunto de n enteros consecutivos mayores a 2. Entonces estos enteros son divisibles por al menos un número primo.

Suponemos cierto el resultado para $k \geq 1$, es decir, existe $m \geq 2$ tal que $m, m+1, \ldots, m+n-1$ son divididos por al menos k primos distintos.

Para $k+1$, sea

$$M = \prod_{i=0}^{n-1}(m+i)^2 = m^2(m+1)^2\cdots(m+n-1)^2$$

y sea $M_1 = M+m$.

Consideremos $M_1, M_1+1, \ldots, M_1+n-1$. Sea $t = M_1+i$, $0 \leq i \leq n-1$. Entonces

$$t = M_1+i = M+n+i = \prod_{j=0}^{n-1}(m+j)^2 + (m+i) = (m+i)\left(\frac{M}{m+i}+1\right).$$

Se tiene que $m+i$ es dividido por al menos k primos distintos.

Por otro lado $m+i|M$, por lo que se tiene que $\dfrac{M}{m+i}+1 \in \mathbb{N}$. Además tenemos que $\left(m+i, \dfrac{M}{m+i}+1\right) = 1$.

Sea q cualquier primo que divide a $m+i$. Entonces t es dividido por al menos $k+1$ primos distintos. ❀

Aquí queremos mencionar que hemos dado la demostración más elemental posible, pero podemos dar demostraciones, también elementales, pero usando el Teorema Chino del Residuo. Por ejemplo podemos considerar, dado que sabemos que hay una infinidad de primos (lo cual ya probamos), que si dados n, k podemos dar n conjuntos cada uno con k primos distintos (siendo los nk primos todos distintos entre sí). Digamos que enumeramos los primos de la siguiente forma: $\{p_{1,1}, p_{1,2}, \ldots, p_{1,k}\}, \ldots, \{p_{n,1}, p_{n,2}, \ldots, p_{n,k}\}$ y más aún escogemos potencias $\alpha_{i,j} \geq 1$ para $1 \leq i \leq n, 1 \leq j \leq k$ y si definimos $A_i := \prod_{j=1}^{k} p_{i,j}^{\alpha_{i,j}}$ para $i = 1, 2, \ldots, n$, entonces puesto que $A_1, \ldots, A_n$ son primos relativos a pares, por el Teorema Chino del Residuo existe $x \in \mathbb{Z}$ tal que

$$\begin{aligned}
x &\equiv 0 \text{ mód } A_1 \\
x &\equiv -1 \text{ mód } A_2 \\
&\vdots \\
x &\equiv -(i-1) \text{ mód } A_i \\
&\vdots \\
x &\equiv -(n-1) \text{ mód } A_n.
\end{aligned}$$

Notemos que $A_i|x+(i-1)$ para $i = 1, \ldots, n$. En particular $x, x+1, \ldots, x+n-1$ son n enteros consecutivos divididos por al menos k primos distintos (y de hecho a cualquier potencia que queramos).

5. Postulado de Bertrand

El *Postulado de Bertrand* establece que dado $n \in \mathbb{N}$, $n \geq 2$, entre n y $2n$ siempre hay un número primo. Equivalentemente, se tiene que si p es primo entonces el siguiente primo q de p satisface $q < 2p$. Notemos este contraste con respecto al Teorema 4.1.

Para ser capaces de dar una demostración del Postulado de Bertrand, necesitamos la siguiente función aritmética.

Definición 5.1 Sea $\vartheta : \mathbb{R}^+ \to \mathbb{R}$, $\vartheta(x) = \sum_{\substack{p \leq x \\ p \text{ primo}}} \log p = \log\left(\prod_{p \leq x} p\right)$.

Para probar esta propiedad, necesitamos:

Proposición 5.2 *Se tiene que* $\vartheta(n) < 2n \log 2$ *para toda* $n \geq 1$.

DEMOSTRACIÓN: Sea $m \in \mathbb{N} \cup \{0\}$.

$$M = \binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!} = \frac{(2m+1)\cdots(m+2)}{m!} \in \mathbb{N}.$$

Ahora $(1+1)^{2m+1} = \sum_{n=0}^{2m+1} \binom{2m+1}{n} > \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2M.$
Por lo tanto se tiene

$$M < 2^{2m}.$$

Si $m+1 < p \leq 2m+1$, $p | (2m+1)\cdots(m+2)$, $p \nmid m!$ por lo que

$$\left(\prod_{m+1<p\leq 2m+1} p\right) | M$$

y

$$\vartheta(2m+1) - \vartheta(m+1) = \sum_{m+1<p\leq 2m+1} \log p \leq \log M < 2m \log 2.$$

Para $n = 1, 2$ el resultado es trivial. Suponemos cierto el resultado para $n \leq n_0 - 1$. Si n_0 es par:

$$\vartheta(n_0) = \vartheta(n_0 - 1) < 2(n_0 - 1)\log 2 < 2n_0 \log 2.$$

Si n_0 es impar, $n_0 = 2m+1$,

$$\begin{aligned} \vartheta(n_0) &= \vartheta(2m+1) = \vartheta(2m+1) - \vartheta(m+1) + \vartheta(m+1) < \\ &< 2m \log 2 + 2(m+1)\log 2 = \\ &= 2(2m+1)\log 2 = 2n_0 \log 2 \end{aligned}$$

puesto que $m + 1 < n_0$. ❀

Teorema 5.3 (Postulado de Bertrand (1845), [15, 6]) *Si* $n \geq 1$, *entonces existe al menos un número primo* p *tal que* $n < p \leq 2n$, *esto es, si* p_r *es el* r*–ésimo primo,* $p_{r+1} < 2p_r$ *para toda* $r \geq 1$.

DEMOSTRACIÓN: Para $n \leq 2^9 = 512$, cada primo de los siguientes

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$

es menor que 2 veces se predecesor. Por lo tanto podemos tomar $n > 2^9$.

Ahora si $p^{\alpha(p)}|n!$, $p^{\alpha(p)+1} \nmid n!$, entonces

$$\alpha(p) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

pues los números $1, 2, \ldots, n$ incluyen exactamente $\left[\frac{n}{p}\right]$ múltiplos p, $\left[\frac{n}{p^2}\right]$ múltiplos de $p^2, \ldots,$ $\left[\frac{n}{p^i}\right]$ múltiplos de p^i.

Sea $N = \dfrac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{k_p}$. Por lo tanto tenemos que

$$k_p = \sum_{m=1}^{\infty} \left(\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right] \right).$$

Sea p un factor primo de N. Por lo tanto $k_p \geq 1$.

Supongamos que no hay ningún primo satisfaciendo $n < p \leq 2n$. Entonces $p \leq n$.

Si $\dfrac{2}{3}n < p \leq n$ entonces $2p \leq 2n < 3p$ y $p^2 > \dfrac{4}{9}n^2 > 2n$. Se sigue que

$$k_p = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 = 0,$$

lo cual es una contradicción. Por lo tanto $p \leq \dfrac{2}{3}n$ para toda $p|N$. De esta forma obtenemos que

$$\sum_{p|N} \log p \leq \sum_{p \leq \frac{2}{3}n} \log p = \vartheta\left(\frac{2}{3}n\right) \leq \frac{4}{3}n \log 2 \quad \text{(Proposición 5.2).}$$

Si $k_p \geq 2$, entonces $k_p = \sum_{m=1}^{\infty} \left(\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right] \right)$.

Cada término $\left(\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right] \right)$ es 1 ó 0 correspondiente a si $\left[\frac{2n}{p^m}\right]$ es impar o par. Para $p^m > 2n$ el término es 0. Se tiene

$$k_p \leq \sum_{\substack{p^m \leq 2n \\ m \log p \leq \log 2n}} 1 \leq \left[\frac{\log 2n}{\log p}\right].$$

Por lo tanto $2\log p \leq k_p \log p \leq \log(2n) \Rightarrow p \leq \sqrt{2n}$. Esto implica que hay a lo más $\sqrt{2n}$ valores de p.

Se sigue que $\sum_{k_p \geq 2} k_p \log p \leq \sqrt{2n}\log(2n)$. Por lo tanto

$$\begin{aligned} \log N &\leq \sum_{k_p=1} \log p + \sum_{k_p \geq 2} k_p \log p \leq \sum_{p|N} \log p + \sqrt{2n}\log(2n) \\ &\leq \frac{4}{3} n \log 2 + \sqrt{2n}\log(2n). \end{aligned}$$

Ahora $(1+1)^{2n} = \sum_{j=0}^{2n} \binom{2n}{j}$ y $\binom{2n}{2n-j} = \binom{2n}{j} \leq \binom{2n}{n} = N$ para toda $0 \leq j \leq n$, por lo tanto

$$\begin{aligned} 2^{2n} \leq 2nN \Rightarrow 2n\log 2 \leq \log 2n + \log N \leq \\ \leq \frac{4}{3} n \log 2 + (1+\sqrt{2n})\log(2n). \end{aligned}$$

Se sigue que $\frac{2}{3} n \log 2 \leq (1+\sqrt{2n})\log(2n)$ lo cual implica $2n\log 2 \leq 3(1+\sqrt{2n})\log(2n)$.

Sea

$$\begin{aligned} \xi &= \frac{\log(n/512)}{10\log 2} > 0 \text{ lo cual implica} \\ \xi &= \frac{\log 2n/2^{10}}{\log 2^{10}} = \frac{\log 2n}{\log 2^{10}} - 1 \text{ por lo tanto} \\ \xi + 1 &= \frac{\log 2n}{\log 2^{10}} \quad \text{o} \quad \log 2^{10(\xi+1)} = \log 2n \text{ de donde se sigue} \\ 2n &= 2^{10(1+\xi)}. \end{aligned}$$

Por lo tanto $2n\log 2 \leq 3(1+\sqrt{2n})\log(2n)$ toma la forma

$$2^{10(1+\xi)} \leq 30(1+\xi)(1+2^{5(1+\xi)}).$$

Se sigue que

$$\begin{aligned} 2^{5\xi} &= 2^{10(1+\xi)} \cdot 2^{-5\xi} \cdot 2^{-10} \leq \\ &\leq 30 \cdot 2^{-5}(1+\xi)(2^{-5-5\xi}+1). \end{aligned}$$

Puesto que $30 \cdot 2^{-5} = \frac{30}{32} < 1 - 2^{-5} = 1 - \frac{1}{32}$ y $(2^{-5-5\xi}+1) < 1 + 2^{-5}$, entonces

$$2^{5\xi} < (1-2^{-5})(1+2^{-5})(1+\xi) = (1-2^{-10})(1+\xi) < 1+\xi.$$

Por lo tanto

$$2^{5\xi} < 1 + \xi.$$

Por otro lado $2^{5\xi} = 2^{5\xi \log 2} > 1 + 5\xi \log 2 > 1 + \xi$, lo cual es absurdo.
❀

Referencias

[1] Cox, David A., *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*, Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, (1989).

[2] de la Vallée-Poussin, Charles Jean, *Recherches analytiques la théorie des nombres premiers*, Ann. Soc. scient. Bruxelles **20**, 183–256 (1896).

[3] Dirichlet, P. G. Lejeune, *Lectures on number theory.* (English summary) Supplements by R. Dedekind. Translated from the 1863 German original and with an introduction by John Stillwell. History of Mathematics, **16**, American Mathematical Society, Providence, RI; London Mathematical Society, London, (1999).

[4] Edwards H.M., *Fermat's Last Theorem*, Springer Verlag GTM **50**, (2000).

[5] Erdös, Paul, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem.* Proc. Nat. Acad. Sci. U.S.A. **35**, 374-379 (1949).

[6] Erdös, Paul, *Beweis eines Satzes von Tschebyschef*, Acta Sci. Math. (Szeged) **5**), 194–198 (1930–1932).

[7] Euclides, *Elements*, Book IX.

[8] Euler, Leonhard, *Variae observations circa series infinitas*, Commentarii academiae scientiarum Petropolitanae **9** (1737), 160–188 (1744). Reprinted in Opera Omnia Series I volume **14**, 216–244 (1925).

[9] Faltings, Gerd, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (3), 349–366 (1983).

[10] Frey, Gerhard, *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1**, 1-40. (1986).

[11] Gauchman, Hillel, *A Special Case of Dirichlet's Theorem on Primes in an Arithmetic Progression*, Math. Mag. **74**, no. 5, 397–399 (2001).

[12] Gauss Carl Friedrich, *Disquisitiones Arithmeticae*. Traducción del latín al español por Hugo Barrantes Campos, Michael Josephy y Ángel Ruiz Zúñiga. Colección *Enrique Pérez Arbelaéz*, **10**, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá, (1995).

[13] Gherardelli, Francesco, *Two famous problems of number theory: the Fermat "theorem" and the Mordell "conjecture" (Italian)*, Archimede **38** (1), 3–9 (1986).

[14] Hadamard, Jacques *"Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques (')"*, Bull. Soc. math. France **24**, 199–220 (1896).

[15] Hardy, Godfrey Harold; Wright, Edward Maitland, *An introduction to the theory of numbers. Fourth edition*, Oxford, at the Clarendon Press, (1960).

[16] Landau, Edmund Georg Hermann, *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig u. Berlin: B. G. Teubner. X (1909). Reimpresión AMS Chelsea Publishing, (2000).

[17] Mordell, Louis Joel, *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees*, Proc. Cambridge Philos. Soc. **21**, 179-192, (1922–23).

[18] Ribet, Kenneth A., *On modular representations of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100**, no. 2, 431–476 (1990).

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

[20] Selberg, Atle, *An Elementary Proof of the Prime Number Theorem*, Ann. Math. (2) **50**, 305–313 (1949).

[21] Shimura, Goro; Taniyama, Yutaka, *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, Tokyo, Mathematical Society of Japan, (1961).

[22] Taylor, Richard; Wiles, Andrew, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141**, no. 3, 553–572 (1995).

[23] Washington, Lawrence C., *Introduction to cyclotomic fields*, Second edition. Graduate Texts in Mathematics, **83**, Springer–Verlag, New York, (1997).

[24] Wiles, Andrew, *Modular forms, elliptic curves, and Fermat's last theorem*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994), 243–245, Birkhäuser, Basel, (1995).

[25] Wiles, Andrew, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141**, no. 3, 443–551 (1995).