Capítulo 1

Números primos y compuestos

En este capítulo consideraremos algunas propiedades del conjunto de los números enteros y positivos: $1, 2, 3, \ldots$ Es costumbre utilizar la letra $\mathbb{N}$ para designar a dicho conjunto, así como $\mathbb{Z}$ es la notación usual en Matemáticas para representar al conjunto de todos los números enteros (positivos, negativos y cero). La aritmética elemental se ocupa del estudio de las operaciones básicas de los enteros, suma, resta y multiplicación y, junto con la Geometría Euclídea, constituye los cimientos y aporta los primeros modelos sobre los que luego se construyen y conforman otras ramas de la Matemática. En los sucesivo supondremos ciertos conocimientos de la Aritmética elemental para pasar directamente a estudiar la relación de divisibilidad.

1.1. El teorema fundamental de la aritmética

Un entero positivo $p > 1$ es un número primo si sus únicos divisores positivos son 1 y p. Por ejemplo los números $2, 3, 5, 7, 11, 13$ son primos. Los enteros positivos mayores que 1 que no son primos se llaman compuestos.

El concepto de número primo se remonta a la antigüedad. Los griegos poseían dicho concepto, así como una larga lista de teoremas y propiedades relacionadas con él. Los cuatro ejemplos siguientes aparecen el *Los Elementos de Euclides*:

- Todo entero positivo, distinto de 1, es un producto de primos.
- Teorema fundamental de la aritmética: Todo entero positivo puede descomponerse de manera única en un producto de primos.
- Existen infinitos números primos.

- Podemos obtener una lista de los números primos por medio del método conocido con el nombre de *Criba de Eratóstenes*.

Estas propiedades justifican la importancia de los números primos y la curiosidad que han inspirado entre los matemáticos de todas las épocas.

Proposición 1.1.1. *Todo entero positivo mayor que* 1 *es un producto de números primos.*

Demostración. Por inducción. La hipótesis es cierta en el caso $n = 2$. Supongámosla cierta para $n \leq m$ y probemos que $m + 1$ es un producto de primos.

Si tenemos tanta suerte que $m + 1$ es primo, entonces no hay nada que demostrar; en caso contrario $m + 1$ se podrá escribir de la forma $m + 1 = n_1 n_2$ con $1 < n_1 \leq n_2 < m + 1$. Por ser n_1 y n_2 menores que $m + 1$ y mayores que 1, ambos serán productos de primos y también lo habrá de ser $m + 1$. □

Sean a y b dos números enteros alguno de los cuales es distinto de 0. El máximo común divisor de a y b es el mayor entero positivo (a, b) que divide a ambos a y b. El caso en que $(a, b) = 1$ recibe un nombre especial, se dice que a y b son primos relativos o primos entre sí. El mínimo común múltiplo $[a, b]$ es el menor entero no negativo que es divisible por a y por b. Si a y b son primos relativos entonces $[a, b] = |ab|$. En general se verifica que $|ab| = (a, b)[a, b]$.

Proposición 1.1.2 (Algoritmo de la división)**.** *Dados dos enteros cualesquiera a y b $(a > 0)$, existen dos únicos enteros q y r tales que $b = aq + r,\ 0 \leq r < a$. Si $a \nmid b$ entonces $0 < r < a$.*

Demostración. Considérese el conjunto $\{b - qa,\ q \in \mathbb{Z}\}$. Sea r el menor número no negativo de la sucesión. Obviamente $r = b - qa$ para algún q. Es claro que $r < a$. En caso contrario $0 \leq b - (q + 1)a = r - a < r$ y entonces r no ya sería el mínimo entero positivo con esa propiedad. La unicidad de r implica la de q. □

Algoritmo de Euclides. *Supongamos que $a > b$ y $a = bc + r,\ a \leq r < b$. Es claro que todo divisor común de a y b lo es también de b y r, y viceversa. En particular $(a, b) = (b, r)$. Esta estrategia puede ser iterada. El último resto distinto de* 0 *es el máximo común divisor de los números a y b.*

Proposición 1.1.3. *Fijados b y c, existen enteros x_0 y y_0 tales que $(b, c) = bx_0 + cy_0$.*

Demostración. Consideremos el menor entero positivo l del conjunto $\{bx + cy : x, y \in \mathbb{Z}\}$. Sea $l = bx_0 + cy_0$. Si $l \nmid b$, existen q y r tales que $b = lq + r,\ 0 < r < l$.

$$r = b - ql = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0).$$

Entonces r pertenece al conjunto, es positivo y menor que l; y eso contradice la elección del entero l. Luego $l \mid b$. Por la misma razón $l \mid c$. Es decir, $l \mid (b, c)$.

Por otra parte $(b, c) \mid b$ y $(b, c) \mid c$. En particular $(b, c) \mid (bx_0 + cy_0)$. Por lo tanto hemos probado que $l = bx_0 + cy_0 = (b, c)$. □

Corolario 1.1.4. *Si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

Demostración. Si $p \nmid a$ entonces $(p, a) = 1$ y, por la proposición anterior, existen x_0, y_0 tales que $1 = px_0 + ay_0$.

Luego $b = bpx_0 + bay_0$. Obviamente $p \mid bpx_0$ y por hipótesis $p \mid bay_0$. De aquí concluimos que $p \mid b$. □

Estamos ahora en condiciones de probar el teorema fundamental de la aritmética.

Proposición 1.1.5 (Teorema Fundamental de la Aritmética)**.** *Todo entero positivo puede descomponerse en producto de números primos de manera única, salvo por una reordenación de los factores.*

Demostración. Consideremos el menor entero $n \geq 2$ para el que no sea cierto. Entonces existirán dos factorizaciones distintas de n,

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} = q_1^{\beta_1} \cdots q_h^{\beta_h}$$

donde todos los primos p_i son distintos de los q_j. En caso contrario podríamos dividir por algún primo común y tendríamos un entero menor que n para el que no se cumpliría el teorema fundamental de la aritmética.

Como p_1 divide a $q_1^{\beta_1} \cdots q_h^{\beta_h}$, por el corolario anterior sabemos que p_1 divide a q_1, lo cual es imposible porque q_1 es primo y distinto de p_1, o divide a $q_1^{\beta_1 - 1} q_2^{\beta_2} \cdots q_h^{\beta_h}$. Iteramos el argumento sucesivamente hasta llegar a una contradicción. □

Observación 1.1.6. *El teorema fundamental de la aritmética puede parecer demasiado obvio. Eso es debido a que el anillo $\mathbb{Z}$ no nos deja ver el bosque de los demás anillos.*

Consideremos por ejemplo el anillo de los enteros $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Los enteros $1 + 2\sqrt{-5}$, $1 - 2\sqrt{-5}$, 3 y 7 son "primos"diferentes en ese anillo y sin embargo $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 3 \cdot 7$.

En este anillo no se cumple el teorema fundamental de la aritmética.

1.2. Algunos resultados acerca de la distribución de los números primos

Mathematicians have tried in vain to discover some order in the sequence of prime numbers but we have every reason to believe that there are some mysteries which the human mind will never penetrate. L. Euler (1770).

La sucesión de los números primos ha interesado a los matemáticos a lo largo de su historia. De una manera sencilla pueden formularse preguntas acerca de este conjunto de números cuya respuesta es muy difícil. Por ejemplo, ¿Existe una fórmula explícita para la función $f(n) = p_n$ =enésimo número primo?, ¿Hay alguna función elemental f tal que $f(n)$ sea primo para todo n?

Es claro que una respuesta positiva a estas preguntas nos daría información acerca de cómo los números primos aparecen en la sucesión de los números naturales.

El polinomio $f(x) = x^2 - x + 41$ toma valores primos para $n = 0, 1, \ldots, 40$, sin embargo $f(41) = 41^2$.

Fermat conjeturó que todos los números de la forma $F_n = 2^{2^n} + 1$ son primos. Los cuatro primeros $F_1 = 5,\ F_2 = 17,\ F_3 = 257$ y $F_4 = 65537$ lo son, pero Euler probó que $F_5 = 641 \cdot 6700417$ es compuesto y, por tanto, que la conjetura de Fermat es falsa. Es más, nadie ha podido encontrar hasta ahora otro primo de Fermat. Pero tampoco nadie ha podido demostrar que hay infinitos números compuestos de Fermat.

El número de Fermat más pequeño para el que no se conoce si es primo o compuesto es F_{33}, y el número compuesto de Fermat más grande que se conoce es $F_{2478782}$, que es divisible por $3 \cdot 2^{2478782} + 1$.

¿Existe para cada entero positivo n un número primo tal que $n < p \leq 2n$?, ¿Es todo número par mayor que dos la suma de dos primos?. La primera de estas preguntas es conocida bajo el nombre de Postulado de Bertrand y fue contestada por Chebychev en 1850. La segunda es la Conjetura de Goldbach y su respuesta nos es aún desconocida.

Otro problema interesante es el de los primos gemelos. Por ejemplo: 3 y 5, 5 y 7, 11 y 13, 17 y 19, 29 y 31 etc. ¿Existen infinitas parejas de primos gemelos? Formulado ya por los griegos, es uno de los problemas más antiguos de la Matemática que, sin embargo, todavía espera su solución.

El resultado básico acerca de la distribución de los números primos es conocido bajo el nombre de Teorema de los Números Primos.

Sea x un número real positivo y designemos con $\pi(x)$ el número de primos

menores o iguales que x; el teorema del número primo consiste en la igualdad:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1. \tag{1.1}$$

Legendre, en 1798, fue el primer matemático que conjeturó la igualdad anterior. Por esas fechas Gauss estaba también interesado en el mismo problema y había construido tablas que incluían todos los primos entre 2 y 3,000,000. Utilizando esta montaña de material experimental Gauss conjeturó que la densidad de primos en un entorno del entero n es $\frac{1}{\log n}$ y, por lo tanto, el número de primos en el intervalo (m, n) debería ser aproximadamente igual a

$$\int_m^n \frac{dx}{\log x}. \tag{1.2}$$

En sus tablas, Gauss encontró que entre 2,600,000 y 2,700,000 existen 6762 primos, mientras que el valor de la integral anterior entre esos dos valores es $6761,332...$

Chebychev, en sus intentos de probar la conjetura de Gauss-Legendre, demostró que existen dos constantes positivas c y C, tales que $0 < c \leq 1 \leq C < \infty$ y

$$c\frac{x}{\log x} \leq \pi(x) \leq C\frac{x}{\log x} \qquad \text{para todo } x \geq 2.$$

Un avance enorme fue dado por B. Riemann quien redactó un famoso artículo acerca de este problema en el año 1850. La idea brillante de Riemann fue conectar el estudio de la función $\pi(x)$ con el de la función $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ (la función zeta de Riemann), definida para valores complejos de s. En particular, el comportamiento asintótico de $\pi(x)$ cuando x tiende a infinito está relacionado con la ubicación de los ceros de la función zeta de Riemann (es decir, los puntos donde se anula esta función)

Sin embargo el plan de Riemann para demostrar el teorema de los números primos no pudo llevarse a acabo hasta mucho más tarde, cuando se dispuso de la teoría de funciones analíticas, de la cual Riemann fue uno de los fundadores y de la que puede afirmarse que buena parte de sus resultados fueron obtenidos para aplicarlos a problemas de la teoría de números. Durante la última década del siglo XIX, Hadamard y de la Vallee Poussin, independientemente, desarrollaron los métodos de Riemann y al teoría de funciones analíticas para conseguir la primera demostración del teorema conjeturado por Gauss y Legendre. Sin embargo, una de las propiedades que Riemann predijo acerca de $\zeta(s)$ permanece todavía sin ser demostrada: la llamada Hipótesis de Riemann que asegura que todos los ceros no reales de la función $\zeta(s)$ tienen parte real $\sigma = 1/2$. Digamos que, cuanto más precisa es la información acerca de los ceros de $\zeta(s)$, tanto más precisa es la estimación que podemos obtener de la diferencia $\left|\pi(x) - \int_2^x \frac{dt}{\log t}\right|$.

La hipótesis de Riemann, junto con el problema $P = NP$ y el problema de Navier-Stokes, constituye la trilogía de problemas abiertos más famosa de la matemática de principios de este siglo.

1.2.1. Desde Euclides hasta Euler

Proposición 1.2.1. *Existen infinitos números primos*

Demostración 1 (Euclides). Supongamos que sólo hay un número finito de primos $p_1, p_2, \ldots, p_n$. Cualquier primo q que divida a $m = p_1 \cdots p_n + 1$ tiene que dividir también a $p_1 \cdots p_n$ y por lo tanto a la diferencia, que es 1. □

Demostración 2 (Polya). Esta demostración está basada en el hecho de que los números de Fermat son primos entre sí. Por lo tanto al menos hay tantos primos como números de Fermat; es decir infinitos.

Si m es par, entonces $\frac{x^m-1}{x+1} = x^{m-1} - x^{m-2} + \cdots - 1$. Para $x = 2^{2^n}$ y $m = 2^k$ tenemos que $\frac{F_{n+k}-2}{F_n} = \frac{x^m-1}{x+1}$ es un entero, luego $F_n \mid F_{n+k} - 2$. Entonces cualquier divisor de F_n y F_{n+k} debe ser también un divisor de $F_{n+k} - 2$ y por lo tanto de 2. Como los F_n son impares necesariamente el único divisor común posible es el 1. □

Demostración 3. Supongamos que existe un número finito de primos $p_1, \ldots, p_k$. Todos los enteros positivos menores que x se tendrían que escribir de la forma $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ para algunos enteros $0 \leq \alpha_i \leq \log x / \log p_i \leq \log x / \log 2$. Entonces el número de posibles $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ menores que x es a lo más $(1 + \log x / \log 2)^k$, que es claramente menor que x si x es suficientemente grande. □

Teorema 1.2.2. *(Euler) La suma de los inverso de los primos es infinita*

$$\sum_p \frac{1}{p} = \infty.$$

Demostración. Euler definió la función $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ para todo número real $s > 1$, y observó la siguiente identidad

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Para demostrar esto último observemos que $\left(1 - \frac{1}{p^s}\right)^{-1} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$ y que al considerar el producto cuando recorremos todos los primos p obtenemos

una suma infinita de la forma $\sum \frac{1}{n^s}$ sobre el 1 y todos los enteros que son producto de potencias de primos. Es decir, sobre todos los enteros positivos. Además, como la factorización en primos es única salvo el orden de los factores, cada n aparece solamente una vez en el sumatorio.

Tomando logaritmos en la identidad tenemos

$$-\sum_p \log\left(1-\frac{1}{p^s}\right) = \log\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right).$$

Ahora tenemos en cuenta que $\log(1-x) \geq -x-2x^2$ para $0 < x \leq 1/2$ para deducir que

$$\sum_p \frac{1}{p^s} \geq \log\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right) - 2\sum_p \frac{1}{p^{2s}}.$$

Cuando $s \to 1$ el segundo sumatorio del segundo término está acotado pero el primero no lo está debido a la divergencia de la serie armónica. Luego la suma de los inversos de los primos tiene que ser también divergente. □

Esta demostración de Euler es un hito en el desarrollo de la teoría y fue la base sobre la que B. Riemann construyó el plan antes mencionado. Que la serie de los recíprocos de los primos sea divergente nos da más información sobre la sucesión de los números primos que el mero hecho de la existencia de infinitos de ellos.

Es el momento de señalar que Viggo Brun demostró que la suma de los inversos de los primos gemelos es convergente,

$$\sum_{p,\ p+2=p'} \frac{1}{p} < +\infty, \tag{1.3}$$

aunque, como mencionamos antes, es un problema abierto saber si existen infinitos de ellos.

1.2.2. El teorema de Chebychev

Aunque el método de Chebychev, de carácter elemental, no fue lo suficientemente poderoso como para demostrar el teorema del número primo, sí lo fue para demostrar que el orden de magnitud de $\pi(x)$ era el que se pronosticaba.

Chebychev observó que los factoriales y los números combinatorios escondían mucha información sobre los números primos. Esto lo podemos apreciar en los dos lemas siguientes, que van a ser piezas claves en la demostración del teorema de Chebychev.

Lema 1.2.3. *Para todo entero positivo $n \geq 2$ se tiene que*

$$\prod_{p \leq n} p < 4^n.$$

Demostración. Lo haremos por inducción sobre n. Es claro para $n = 2$ y supongamos que es cierto para todo entero menor que n.

Si n es par, claramente $\prod_{p \leq n} p = \prod_{p \leq n-1} p < 4^{n-1} < 4^n$.

Si $n = 2k + 1$ es impar, la observación crucial es que el producto

$$\prod_{k+1 < p \leq 2k+1} p$$

divide (y como consecuencia es menor) al número combinatorio

$$\binom{2k+1}{k+1} = \frac{(2k+1)(2k)\cdots(k+2)}{1 \cdots k}$$

ya que cada primo involucrado en el producto divide al numerador pero no al denominador.

Por otra parte, como el número combinatorio $\binom{2k+1}{k+1} = \binom{2k+1}{k}$ aparece dos veces en el desarrollo de $(1+1)^{2k+1}$, es en particular menor o igual que 4^k, la mitad del valor de esta última expresión. Finalmente utilizamos la hipótesis de inducción para llegar a

$$\prod_{p \leq n} p = \prod_{p \leq k+1} p \prod_{k+1 < p \leq 2k+1} p < 4^{k+1} 4^k = 4^{2k+1} = 4^n.$$

□

Lema 1.2.4 (Legendre)**.** *El exponente del primo p en al factorización de $n!$ es exactamente*

$$\sum_k \left\lfloor \frac{n}{p^k} \right\rfloor$$

Demostración. Para todo x real llamemos $e_p(x)$ al exponente de p en $\lfloor x \rfloor ! = 1 \cdot 2 \cdots \lfloor x \rfloor$. Ya que sólo los múltiplos de p en este producto colaboran en el exponente $e_p(x)$, si escribimos el producto de estos múltiplos como $p \cdot (2p) \cdots (\lfloor \frac{x}{p} \rfloor p) = p^{\lfloor \frac{x}{p} \rfloor} \lfloor \frac{x}{p} \rfloor !$ podemos ver que

$$e_p(x) = \left\lfloor \frac{x}{p} \right\rfloor + e_p\left(\frac{x}{p}\right) = \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + e_p\left(\frac{x}{p^2}\right) = \cdots = \sum_k \left\lfloor \frac{x}{p^k} \right\rfloor.$$

□

Corolario 1.2.5. *El exponente de p en $\binom{2n}{n}$ es*

$$s_p = \sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right) \leq \left\lfloor \frac{\log(2n)}{\log p}\right\rfloor.$$

Demostración. Es consecuencia inmediata del lema anterior y de la observación de que $[2y]-2[y]$ es 0 o 1 para todo $y>0$. La desigualdad se deduce del hecho de que si $k > \log(2n)/\log p$, todas las partes enteras involucradas valen cero. □

Teorema 1.2.6 (Chebychev)**.** *Existen constantes positivas $0 < c \leq 1 \leq C < \infty$ tales que para todo $x \geq 2$,*

$$c\frac{x}{\log x} \leq \pi(x) \leq C\frac{x}{\log x}. \tag{1.4}$$

Demostración. Separando los primos menores que $\sqrt{n}$ en el lema 1.2.2 tenemos que

$$(\sqrt{n})^{\pi(n)-\pi(\sqrt{n})} \leq \prod_{\sqrt{n}<p\leq n} p \leq 4^n.$$

Tomando logaritmos y observando que $\pi(\sqrt{n}) \leq \sqrt{n}$ vemos que

$$\pi(n) \leq (2\log 4)\frac{n}{\log n} + \pi(\sqrt{n}) \leq \left(2\log 4 + \frac{\log n}{\sqrt{n}}\right)\frac{n}{\log n} \leq 4\frac{n}{\log n}.$$

Para la cota inferior observemos primero que, como $\binom{2n}{n}$ es el término más grande de los $2n+1$ términos del desarrollo de Newton de $(1+1)^{2n}$ entonces,

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n}. \tag{1.5}$$

El corolario 1.2.5 nos permite deducir que

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq \prod_{p\leq 2n} p^{\log(2n)/\log p} = (2n)^{\pi(2n)}.$$

Tomando logaritmos,

$$\pi(2n) \geq \frac{(2\log 2)n - \log(2n+1)}{\log(2n)}.$$

Finalmente, para cualquier número real x se obtiene

$$\pi(x) \geq \pi(2[x/2]) \geq \frac{(2[x/2]+1)\log 2 - \log(2[x/2]+1)}{\log(2[x/2])} \tag{1.6}$$

$$\geq \frac{(x-1)\log 2 - \log(x+1)}{\log x}. \tag{1.7}$$

Esta última cantidad es mayor que $\frac{x}{2\log x}$ para todo $x > 100$, y para los $x \leq 100$ se puede comprobar a mano que también es cierto que $\pi(x) \geq \frac{x}{2\log x}$.

□

Teorema 1.2.7 (Postulado de Bertrand)**.** *Para todo $n > 1$ existe un número primo p tal que $n < p < 2n$.*

Demostración. Empecemos demostrando que si $\frac{2}{3}n < p \leq n$ entonces $s_p = 0$, donde s_p era el exponente de p en $\binom{2n}{n}$. Como $p^2 > 2n$, todas las partes enteras de los términos del sumatorio en el corolario 1.2.5 se anulan si $k \geq 2$. Es decir, $s_p = \left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor$. Pero en el rango que nos ocupa $\left\lfloor \frac{2n}{p} \right\rfloor = 2$ y $\left\lfloor \frac{n}{p} \right\rfloor = 1$.

Por lo tanto, si no hubiera ningún primo p tal que $n < p < 2n$, tendríamos

$$\begin{aligned} \frac{4^n}{2n+1} \leq \binom{2n}{n} &= \prod_{p \leq 2n/3} p^{s_p} \\ &= \prod_{p \leq \sqrt{2n}} p^{s_p} \prod_{\sqrt{2n} < p \leq 2n/3} p^{s_p} \\ &\leq \prod_{p \leq \sqrt{2n}} (2n) \prod_{\sqrt{2n} < p \leq 2n/3} p \\ &\leq (2n)^{\sqrt{2n}} 4^{2n/3}, \end{aligned}$$

donde en el penúltimo paso hemos utilizado el corolario 1.2.5 y en el último, el lema 1.2.2.

Tomando logaritmos llegamos a la desigualdad

$$\frac{\log 4}{3} \leq \frac{\sqrt{2}\log(2n)}{\sqrt{n}} + \frac{\log(2n+1)}{n}$$

que es falsa para $n \geq 500$. Para los $n < 520$ observemos que al sucesión de primos $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521$ tienen la propiedad de que cada uno es mayor que su antecesor pero menor que su doble. □

En una memoria publicada en el año 1850 Chebychev introdujo la función:

$$\Theta(x) = \sum_{p \leq x} \log p,$$

donde la suma está tomada tomada sobre todos los primos p menores o iguales que x, y Riemann, en su famosa memoria por razones técnicas que se entenderán más tarde, consideró la función

$$\Psi(x) = \sum_{p^m \leq x} \log p$$

donde en este caso la suma está extendida sobre todas las combinaciones de un primo p con un entero positivo m, tales que $p^m \leq x$.

Teorema 1.2.8. *Los tres cocientes*

$$\frac{\Theta(x)}{x}, \qquad \frac{\Psi(x)}{x}, \qquad \frac{\pi(x)}{x/\log x}$$

tienen los mismos límites de indeterminación cuando $x \to \infty$.

Demostración. Sean

$$A_1 = \limsup_{x\to\infty} \frac{\Theta(x)}{x}, \quad A_2 = \limsup_{x\to\infty} \frac{\Psi(x)}{x}, \quad A_3 = \limsup_{x\to\infty} \frac{\pi(x)}{x/\log x}$$
$$a_1 = \liminf_{x\to\infty} \frac{\Theta(x)}{x}, \quad a_2 = \liminf_{x\to\infty} \frac{\Psi(x)}{x}, \quad a_3 = \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x}.$$

Tenemos que

$$\Theta(x) \leq \Psi(x) = \sum_{p\leq x} \log p \sum_{\substack{m,\\ p^m\leq x}} 1 \leq \sum_{p\leq x} \log p \left\lfloor \frac{\log x}{\log p} \right\rfloor \leq (\log x)\pi(x).$$

Por lo tanto $\frac{\Theta(x)}{x} \leq \frac{\Psi(x)}{x} \leq \frac{\pi(x)}{x/\log x}$ para todo x. Es decir, $A_1 \leq A_2 \leq A_3$.

Por otro lado, consideramos la función auxiliar $\epsilon(x) = \frac{2\log\log x}{\log x}$, que en particular satisface que $x^{\epsilon(x)} = \log^2 x$ y tenemos que

$$\Theta(x) \geq \sum_{x^{1-\epsilon(x)}<p\leq x} \log p \geq \left(\pi(x) - \pi(x^{1-\epsilon(x)})\right) \log(x^{1-\epsilon(x)}).$$

Y como $\pi(x^{1-\epsilon}) \leq x^{1-\epsilon(x)}$, obtenemos la relación

$$\frac{\Theta(x)}{x} \geq (1-\epsilon(x)) \left(\frac{\pi(x)}{x/\log x} - \frac{\log x}{x^{\epsilon(x)}} \right) \geq (1-\epsilon(x)) \frac{\pi(x)}{x/\log x} - \frac{1}{\log x}.$$

Tomando límites superiores obtenemos que $A_3 \geq A_1$. Por tanto $A_1 = A_2 = A_3$. La identidad $a_1 = a_2 = a_3$ se demuestra de manera análoga.

□

1.3. Ejercicios del capítulo 1

1.3.1. *D. Pedro le dijo a D. Sixto: Tengo tres hijas, el producto de sus edades es* 36*, y la suma el número de tu portal.*

– *Me falta un dato, dijo D. Sixto.*

– *Tienes razón. La mayor toca el piano, aclaró D. Pedro.*

¿Qué edades tenían las hijas de D. Pedro?

1.3.2. *La Real Sociedad Matemática Española todos los años invita a sus socios a su congreso anual. Este año el* $27,181818..\,\%$ *de los asistentes eran mujeres, el* $55,555...\,\%$ *eran mayores de* 30 *años y el* $37\,\%$ *llevaron algún libro de matemáticas. Sabiendo que el número de socios no es mayor que* 15,000*, ¿Podrías calcular el número de asistentes?*

1.3.3. *Determinar una condición necesaria y suficiente para que la suma de los* n *primeros números naturales divida a su producto.*

1.3.4. *Encontrar todas las ternas de enteros positivos* a, b, c *tales que* $(a, b, c) = 10$ *y* $[a, b, c] = 100$*.*

1.3.5. *Probar que* $(a^2, b^2) = (a, b)^2$*.*

1.3.6. *Probar que si* $(a, b) = 1$ *y* ab *es un cuadrado, entonces* a *y* b *también son cuadrados.*

1.3.7. *Demostrar que* $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$ *para todo* a *y* b*.*

1.3.8. *He comprado bolígrafos a* 101 *pesetas y rotuladores a* 140 *pesetas. Si me he gastado en total* 2993 *pesetas, ¿cuántos he comprado de cada?*

1.3.9. *Dar una condición necesaria y suficiente para que con dos cántaras de* m *y* n *litros se puedan medir* l *litros a la orilla de un rio.*

1.3.10. *Sea* S *un conjunto de* n *enteros no necesariamente distintos. Demostrar que algún subconjunto no vacío de* S *posee una suma divisible por* n*.*

1.3.11. *Demostrar que todo* n *primo con* 10 *tiene infinitos múltiplos cuyos dígitos en base* 10 *son todos unos.*

1.3.12. *Demostrar que si* 5^n *y* 2^n *empiezan por la misma cifra en su expresión decimal, entonces dicha cifra es* 3*.*

1.3.13. *Sea* r *un entero positivo. Demostrar que*

$$\sum_{k=1}^{n} k^r = \frac{n^{r+1}}{r+1} + Q_r(n),$$

donde $Q_r(n)$ *es un polinomio de grado* r *con coeficientes racionales.*

1.3.14. *Demostrar que* $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ *para todo* $n \geq 1$. *Demostrar por inducción que* $p_n \leq 2^{2^n}$. *Deducir que* $\pi(x) \geq \log_2 \log_2 x - 1$, $x \geq 2$.

1.3.15. *Demostrar que existen infinitos primos de la forma* $4n+3$ *y de la forma* $6n+5$.

1.3.16. *Demostrar que* $F_n = \prod_{i=0}^{n-1} F_i + 2$. *Deducir que* $(F_m, F_n) = 1$ *para* $n \neq m$ *y de aquí la existencia de infinitos primos.*

1.3.17. *Demostrar que para todo* $\alpha > 0$ *y para todo* $\epsilon > 0$, *existen* a, b *tales que* $|\frac{a}{b} - \alpha| < \epsilon$ *y* $a + b$ *es primo. Demostrar que este resultado es equivalente a la existencia de infinitos números primos.*

1.3.18. *Demostrar que si* $2^n + 1$ *es primo, entonces* n *es cero o una potencia de* 2.

1.3.19. *Demostrar que si* $2^n - 1$ *es primo,* n *ha de ser primo.*

1.3.20. *Demostrar que* $n^4 + 4$ *sólo es primo para* $n = 1$.

1.3.21. *Demostrar que un polinomio* $P(n)$ *con coeficientes enteros no puede ser primo para todo* n.

1.3.22. *Sea* $\alpha = \sum_{n \geq 1} \frac{p_n}{10^{n^2}}$, *donde* p_n *es el primo enésimo. Demostrar que* α *tiene la propiedad de que* $p_m = [10^{m^2}\alpha] - 10^{2m-1}[10^{(m-1)^2}\alpha]$ *para todo* m.

1.3.23. *Demostrar que* $\limsup_{n\to\infty} p_{n+1} - p_n = \infty$, *donde* p_n *denota el primo n-ésimo. De otra manera, demostrar que para todo* k, *existen* k *números compuestos consecutivos.*

1.3.24. *Sea* $\pi_2(x)$ =*número de primos gemelos menores o iguales que* x. *Sabiendo que* $\pi_2(x) < C\frac{x}{\log^2 x}$ *para alguna constante positiva* C, *demostrar que la suma de los inversos de los primos gemelos converge.*

1.3.25. *Demostrar que para todo* $x \geq 2$,

$$\sum_{p \leq x} \frac{1}{p} \geq \log\log x - 10.$$

1.3.26. *Demostrar, utilizando el teorema de Chebychev, que si* $n > 6$ *entonces* n *puede escribirse como suma de primos distintos.*

1.3.27. *Demostrar, utilizando el teorema de Chebychev, que si* $n > 1$, *entonces* $n!$ *no puede ser una k-potencia.*

1.3.28. *Probar que* $\sum_{j=1}^{n} \frac{1}{j}$ *no es entero si* $n > 1$.

1.3.29. *¿En cuántos ceros acaba* $371!$*?*

1.3.30. *Hallar todos los primos* p *tales que* $p, p+4, p+6, p+10, p+12, p+16$ *y* $p+22$ *sean primos.*

1.3.31. *Un cuadrado de* $n \times n$ *números enteros se dice que es mágico si la suma de los números de cada una de sus filas o columnas, así como de cada una de las dos diagonales principales, es el mismo. Encontrar un cuadrado mágico* 3×3 *formado todo por números primos.*

1.3.32. *Probar que existen dos constantes positivas* c *y* C *tales que*

$$cn \log n < p_n < Cn \log n,$$

para todo n*, donde* p_n *es el primo enésimo.*

1.3.33. *Demostrar que*

$$\log 2 \leq \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} \leq \limsup_{x\to\infty} \frac{\pi(x)}{x/\log x} \leq 2 \log 2.$$

1.3.34. *Mejorar alguna de las cotas del problema anterior utilizando otros números combinatorios.*

En los ejercicios siguientes utilizamos la notación $f(x) \sim g(x)$ para indicar que $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

1.3.35. *Demostrar que* $p_n \sim n \log n$ *es equivalente al teorema del número primo.*

1.3.36. *Sea la función* $Li(x) = \int_2^x \frac{dt}{\log t}$*. Demostrar que* $Li(x) \sim x/\log x$.

1.3.37. *Demostrar que el teorema del número primo es equivalente a que*

$$\log[1, 2, \ldots, n] \sim n.$$

Capítulo 2

Funciones aritméticas

En el capítulo anterior hemos podido apreciar algunos aspectos de la Teoría de los Números y el tipo de problemas que pretende resolver. Ne debe extrañar que ciertas funciones definidas sobre los naturales tengan en ella una importancia capital, tanto por su utilidad como por ser un objeto de estudio en sí mismas.

Estas funciones, reales o complejas, son las funciones aritméticas.

2.1. Funciones aritméticas más comunes

2.1.1. Propiedades generales

Dentro de todas las funciones aritméticas hay unas que merecen especial atención por la importancia de sus propiedades y porque engloban a la mayoría de las funciones aritméticas interesantes: son las funciones multiplicativas.

Definicion 2.1.1. *Diremos que una función f es multiplicativa si $f(nm) = f(n)f(m)$ siempre que $(n, m) = 1$.*

Definicion 2.1.2. *Diremos que una función f es completamente multiplicativa si $f(nm) = f(n)f(m)$ para todo n, m.*

Observemos que si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y f es una función multiplicativa entonces

$$f(n) = \prod_i f(p_i^{\alpha_i}).$$

Proposición 2.1.3. *Si $f(n)$ es una función multiplicativa entonces $g(n) = \sum_{d|n} f(d)$ también lo es.*

Demostración. Observemos que si $(m,n)=1$, todo divisor d de mn ha de ser de la forma $d=d_1d_2$ donde d_1 y d_2 han de ser divisores de m y n respectivamente. De igual manera, cada pareja de divisores de m y n nos da un divisor de mn. Entonces tenemos

$$g(mn)=\sum_{d|mn} f(d)=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1d_2)=\left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right)=g(m)g(n).$$

□

Ahora centraremos nuestra atención sobre las funciones aritméticas más interesantes, empezando con la función divisor.

2.1.2. La función divisor

La función divisor $d(n)$ se define como el número de divisores de n:

$$d(n)=\sum_{d|n} 1.$$

Si $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, los divisores de n son de la forma $d=p_1^{\beta_1}\cdots p_r^{\beta_r},\ 0\le\beta_i\le\alpha_i,\ i=1,\ldots,r$.

Proposición 2.1.4. *La función $d(n)$ es multiplicativa.*

Demostración. Es una consecuencia inmediata de la proposición 2.1.3 □

Corolario 2.1.5. *Si $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ entonces $d(n)=\prod_i(1+\alpha_i)$.*

Demostración. Como la función divisor es multiplicativa entonces $d(n)=\prod_i d(p_i^{\alpha_i})=\prod_i(1+\alpha_i)$. □

2.1.3. La función σ, los números perfectos y los primos de Mersenne

La función σ se define de la forma

$$\sigma(n)=\sum_{d|n} d.$$

Como la función $f(n)=n$ es multiplicativa, el siguiente resultado se sigue también de la proposición 2.1.3.

Proposición 2.1.6. *La función σ es multiplicativa.*

Proposición 2.1.7. *Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, entonces*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Demostración. Al ser σ una función multiplicativa es suficiente demostrar que $\sigma(p_i^{\alpha_i}) = \frac{p_1^{\alpha_i+1}-1}{p_i-1}$.

$$\sigma(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

□

Con la función σ está relacionado el clásico problema de los números perfectos.

Decimos que un entero positivo n es perfecto si la suma de sus divisores menores que n coincide con n. Es decir, si $\sigma(n) = 2n$. El primer número perfecto es el 6 cuyos divisores son $1, 2, 3$ y 6. El siguiente es $28 = 1 + 2 + 4 + 7 + 14$.

El siguiente teorema caracteriza los números pares perfectos.

Teorema 2.1.8. *Un número par es perfecto si y sólo si $n = 2^{m-1}(2^m - 1)$ con $2^m - 1$ primo.*

Demostración. Si $2^m - 1$ es primo entonces $\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1)2^m = 2n$ y n es un número perfecto.

Por otro lado, si n es par, n se puede escribir de la forma $n = 2^{m-1}s$ con s impar y $m \geq 2$. Por ser n un número perfecto tenemos que

$$2^m s = 2m = \sigma(n) = \sigma(2^{m-1})\sigma(s) = (2^m - 1)\sigma(s).$$

Entonces $\sigma(s) = s + \frac{s}{2^m-1}$. Como $\sigma(s)$ es un entero, $2^m - 1$ tiene que ser un divisor de s y por lo tanto $\frac{s}{2^m-1}$ también.

Ya que $\sigma(s)$ es la suma de todos los divisores de s, entonces s y $\frac{s}{2^m-1}$ han de ser los únicos divisores de s. Es decir $\frac{s}{2^m-1} = 1$ y además s tiene que ser primo. □

Aunque en este teorema han quedado perfectamente caracterizados los números perfectos pares, es un problema abierto responder a la pregunta de si existen infinitos números pares perfectos, que es lo mismo que responder sobre la existencia de infinitos primos de la forma $2^m - 1$, los llamados primos de Mersenne.

También se desconoce la existencia de números perfectos impares. No se ha encontrado ninguno pero no se ha demostrado que no existan.

2.1.4. La función de Moebius

Una de las funciones aritméticas más importantes en la teoría analítica de los números es la función de Moebius. Aunque la primera definición de la función pueda resultar algo articial en un principio, aparece de manera natural cuando, por ejemplo, se trata de contar el número de primos menores que una cantidad dada. Esto lo veremos posteriormente.

La función de Moebius $\mu(n)$ se define de la siguiente manera:

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ es el producto de } k \text{ primos distintos} \\ 0 & \text{si } n \text{ tiene algún divisor cuadrado mayor que 1.} \end{cases}$$

Proposición 2.1.9. *La función $\mu(n)$ es multiplicativa.*

Demostración. Si $(m, n) = 1$ entonces $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$ con los p_i distintos de los q_j.

Si alguno de los α_i o de los β_j es mayor que 1, entonces m o n tienen algún divisor cuadrado que también lo será de mn. En este caso $\mu(mn) = \mu(m)\mu(n) = 0$.

Si $\alpha_1 = \cdots = \alpha_r = \beta_1 = \cdots = \beta_s = 1$ entonces $\mu(m) = \mu(p_1 \cdots p_r) = (-1)^r$, $\mu(n) = \mu(q_1 \cdots q_s) = (-1)^s$ y $\mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s}$. □

Proposición 2.1.10.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & si\ n = 1 \\ 0, & si\ n > 1 \end{cases} .$$

Demostración. Al ser $\mu(n)$ multiplicativa, la función $g(n) = \sum_{d|n} \mu(d)$ también lo es y por lo tanto, si $n > 1$, $g(n) = \prod_{p|n} g(p^\alpha$. Pero si p es primo, $g(p^\alpha) = \sum_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^\alpha) = 1 - 1 + 0 + \cdots + 0 = 0$. □

2.1.5. La función de Euler

La función $\phi(n)$ se define como el número de enteros positivos primos con n y menores o iguales que n.

Proposición 2.1.11. *La función $\phi(n)$ es multiplicativa.*

Demostración. Por la proposición 2.1.10, la función $\phi(n)$ también se puede escribir como

$$\phi(n) = \sum_{k \le n} \sum_{d|(k,n)} \mu(d).$$

Reordenando las sumas tenemos

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d}.$$

La demostración se termina con la observación de que al ser $\mu(d)$ multiplicativa, también lo es $\frac{\mu(d)}{d}$. Entonces la función $\frac{\phi(n)}{n}$, y por tanto la función $\phi(n)$, es multiplicativa. □

Corolario 2.1.12.

$$\phi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

Demostración. Solamente hay que observar que $\frac{\phi(n)}{n}$ es multiplicativa y que $\frac{\phi(p^\alpha)}{p^\alpha} = \frac{p^\alpha - p^{\alpha-1}}{p^\alpha} = 1 - \frac{1}{p}$. □

Proposición 2.1.13.

$$\sum_{d|n}\phi(d) = n.$$

Demostración. La función $g(n) = \sum_{d|n}\phi(d)$ es multiplicativa. Por lo tanto sólo hay que demostrar que $g(p^m) = p^m$ para todo primo p y para todo entero positivo m, Esto es,

$$\begin{aligned} g(p^m) &= \sum_{d|p^m}\phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^m) = \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^m - p^{m-1}) = p^m. \end{aligned}$$

□

2.1.6. Promedio de funciones aritméticas

En general, las funciones aritméticas se comportan de un modo bastante irregular. Los valores $d(n)$, $\phi(n)$, $\mu(n)$ no dependen tanto de la magnitud de n como de su factorización en números primos.

Tiene por tanto mayor sentido preguntarse por el comportamiento de dichas funciones en media. Veremos por ejemplo que

$$D(x) = \sum_{n\leq x} d(n) \sim x\log x$$

y que

$$\Phi(x) = \sum_{n \leq x} \phi(n) \sim \frac{\pi^2}{6} x^2.$$

El siguiente teorema va a ser una herramienta importante para estimar sumas por medio de integrales.

Teorema 2.1.14 (Identidad de Abel)**.** *Para toda función aritmética $a(n)$, sea $A(x) = \sum_{n \leq x} a(n)$ y sea f una función con derivada continua en $[1, \infty)$. Entonces tenemos*

$$\sum_{n \leq x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t) dt.$$

Demostración. Utilizaremos el hecho de que $a(n) = A(n) - A(n-1)$ y que $f(n) - f(n-1) = \int_{n-1}^{n} f'(t)dt$. Definimos también $a(0) = 0$ y $k = \lfloor x \rfloor$.

$$\begin{aligned}
\sum_{1 \leq n \leq k} a(n) f(n) &= \sum_{1 \leq n \leq k} (A(n) - A(n-1)) f(n) \\
&= \sum_{1 \leq n \leq k} A(n) f(n) - \sum_{0 \leq n \leq k-1} A(n) f(n+1) \\
&= \sum_{1 \leq n \leq k-1} A(n) \left(f(n) - f(n-1)\right) + A(k) f(k) \\
&= -\sum_{1 \leq n \leq k-1} A(n) \int_n^{n+1} f'(t) dt + A(k) f(k) \\
&= -\int_1^k A(t) f'(t) dt + A(x) f(x) - \int_k^x A(t) f'(t) dt \\
&= A(x) f(x) - \int_1^x A(t) f'(t) dt.
\end{aligned}$$

□

En los cálculos posteriores nos va a interesar el orden de magnitud de algunas funciones más que su valor exacto. Para ello introducimos la siguiente notación:

Notación:

a) $f(x) = O(g(x))$ cuando $x \to \infty$ si existe una constante positiva C tal que $|f(x)| \leq C|g(x)|$ para x suficientemente grande.

b) $f(x) = o(g(x))$, cuando $x \to \infty$ si $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0$.

Análogamente se definen $f(x) = O(g(x))$ y $f(x) = o(g(x))$ cuando $x \to x_0$.

También usaremos la notación $f(x) \ll g(x)$ y la notación $f(x) \gg g(x)$ para indicar que existe una constante positiva C tal que $f(x) \leq Cg(x)$ y $f(x) \geq Cg(x)$ respectivamente.

2.1.7. La constante de Euler

Proposición 2.1.15.

$$\sum_{k=1}^{n} \frac{1}{k} = \log n + \gamma + O(1/n),$$

donde γ es la constante de Euler.

Demostración. Aplicaremos la identidad de Abel a la función aritmética más sencilla de todas, $a(n) = 1$, y a la función $f(x) = \frac{1}{x}$ para estimar las sumas parciales de la serie armónica.

Dichas funciones cumplen las condiciones de la identidad de Abel con $A(x) = \lfloor x \rfloor$ y $f'(x) = -\frac{1}{x^2}$. Tenemos entonces que

$$\begin{aligned} \sum_{k=1}^{n} \frac{1}{k} &= \frac{A(n)}{n} + \int_1^n \frac{A(t)}{t^2} dt = 1 + \int_1^n \frac{t - (t)}{t^2} dt \\ &= 1 + \log n - \int_1^\infty \frac{(t)}{t^2} dt + \int_n^\infty \frac{(t)}{t^2} dt. \end{aligned}$$

Observemos que la última integral es $O\left(\frac{1}{n}\right)$. Entonces

$$\lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n \right) = 1 - \int_1^\infty \frac{(t)}{t^2} dt.$$

Esta constante es la llamada de Euler:

$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n \right).$$

□

La constante de Euler es una de las constantes, como π y como e, que aparecen de una manera natural en las matemáticas. Sin embargo se desconoce, por ejemplo, si γ es un número racional o irracional.

2.1.8. Fórmulas de Mertens

Teorema 2.1.16.

$$a) \qquad \sum_{p\le x}\frac{\log p}{p} = \log x + O(1), \qquad x\to\infty$$

$$b) \qquad \sum_{p\le x}\frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right), \qquad x\to\infty$$

Demostración. En la prueba de estas leyes asintóticas vamos a utilizar la fórmula

$$\log(m!) = m\log m - m + O(\log m),$$

que la podemos deducir comparando $\log(m!)$ con la integral $\int_1^m \log t dt = m\log m - m$, ya que la diferencia

$$\left|\sum_{k=1}^{m}\log k - \int_1^m \log t dt\right| \le \sum_{k=1}^{m}\left|\log k - \int_{k-1}^{k}\log t dt\right|$$
$$\le \sum_{k=2}^{m}|\log k - \log(k-1)| \le \sum_{k=1}^{m} O(1/k) = O(\log m)$$

a) Por el lema 1.2.4 sabemos que $m! = \prod_{p\le m} p^{\alpha_p}$, donde $\alpha_p = \lfloor \frac{m}{p}\rfloor + \lfloor\frac{m}{p^2}\rfloor + \cdots$.

Tomando logaritmos obtenemos la relación:

$$\begin{aligned}\log(m!) &= \sum_{p\le m}\left\lfloor\frac{m}{p}\right\rfloor\log p + \sum_{p\le m}\left(\sum_{k\ge 2}\left\lfloor\frac{m}{p^k}\right\rfloor\log p\right)\\ &= m\sum_{p\le m}\frac{\log p}{p} + \sum_{p\le m}\left(\left\lfloor\frac{m}{p}\right\rfloor - \frac{m}{p}\right)\log p + O(m)\\ &= m\sum_{p\le m}\frac{\log p}{p} + O\left(\sum_{p\le m}\log p\right) + O(m).\end{aligned}$$

Teniendo en cuenta que $\log(m!) = m\log m + O(m)$ y que $\sum_{p\le m}\log p \le (\log m)\pi(m) = O(m)$, resulta que:

$$m\log m + O(m) = m\sum_{p\le m}\frac{\log p}{p} + O(m).$$

Es decir,

$$\sum_{p\le m}\frac{\log p}{p} = \log m + O(1).$$

b) La segunda suma la escribimos de la forma

$$\sum_{p\leq x}\frac{1}{p}=\sum_{p\leq x}\frac{1}{\log p}\frac{\log p}{p}=\sum_{n\leq x}\frac{1}{\log n}a(n),$$

donde $a(n)=\frac{\log p}{p}$ si n es primo y $a(n)=0$ en caso contrario.

Estamos en condiciones de aplicar el lema de sumación de Abel:

$$\sum_{p\leq x}\frac{1}{p}=\frac{1}{\log x}A(x)+\int_2^x\frac{A(t)}{t(\log t)^2}dt,$$

donde

$$A(t)=\sum_{n\leq t}a(n)=\sum_{p\leq t}\frac{\log p}{p}=\log t+O(1)$$

por el resultado anterior.

Tenemos que:

$$\int_2^x\frac{A(t)}{t(\log t)^2}dt=\int_2^x\frac{dt}{t\log t}+\int_2^x\frac{A(t)-\log t}{t(\log t)^2}dt=I_1+I_2.$$

$$\begin{aligned}I_1 &= \int_2^x\frac{dt}{t\log t}=\log\log x-\log\log 2.\\ I_2 &= \int_2^\infty\frac{A(t)-\log t}{t(\log t)^2}dt-\int_x^\infty\frac{O(1)}{t(\log t)^2}dt\\ &= \int_2^\infty\frac{A(t)-\log t}{t(\log t)^2}dt+O\left(\frac{1}{\log x}\right).\end{aligned}$$

Por lo tanto,

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+B+O\left(\frac{1}{\log x}\right),$$

donde

$$B=1-\log\log 2+\int_2^\infty\frac{A(t)-\log t}{t(\log t)^2}dt.$$

□

Observación 2.1.17. *Puede demostrarse que la constante B tiene la forma siguiente:*

$$B=\gamma+\sum_p\left\{\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right\},$$

donde γ es la constante de Euler.

2.1.9. La función $r(n)$. Puntos de coordenadas enteras sobre circunferencias

Dado un entero positivo n, se define $r(n)$ como el número de sus representaciones como suma de dos cuadrados.

$$r(n) = \#\{n = t^2 + s^2 : \ s, t \in \mathbb{Z}\}.$$

Por ejemplo $1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2$ y, por tanto $r(1) = 4$. De igual manera tenemos $r(2) = 4$, $r(3) = 0$, $r(4) = 4$, $r(5) = 8$, $r(6) = 0$, $r(7) = 0$, $r(8) = 4$, etc..

Basta echar una ojeada a una tabla de valores de $r(n)$ para percibir su carácter irregular. Por ello es razonable definir la función

$$R(n) = \sum_{k=1}^{n} r(k)$$

de tal manera que $\frac{R(n)}{n}$ sea un promedio de $r(k)$ y esperar que esta nueva función tenga una distribución de valores más regular.

Ambas funciones tienen una representación muy sencilla en trminos del retículo fundamental:

$r(n)$ = número de puntos del retículo $\mathbb{Z}^2$(de coordenadas enteras) que están situados sobre la circunferencia de radio $\sqrt{n}$ y centro el origen.

$R(n)$ = número de puntos de coordenadas enteras situados en el círculo de centro el origen y radio $\sqrt{n}$.

El siguiente resultado, debido a Gauss, nos da el orden de magnitud de la función $R(n)$ para valores grandes del entero n.

Teorema 2.1.18.

$$R(n) = \pi n + O(\sqrt{n}).$$

Demostración. A cada punto ν de coordenadas enteras le asociamos el cuadrado de área uno, Q_ν, que le tiene como vértice suroeste. El número $R(n)$ es igual al área de la región F del plano formada por la unión de los cuadrados Q_ν tales que ν está dentro del círculo $x^2 + y^2 \leq n$.

Este área no es exactamente igual al área del círculo de radio $\sqrt{n}$, pues algunos de los cuadrados escogidos tienen parte fuera del círculo, mientras que quedan porciones dl círculo sin recubrir.

Sin embargo podemos trazar dos círculos C_1 y C_2 centrados en el origen y de radios respectivos $\sqrt{n} - \sqrt{2}$ y $\sqrt{n} + \sqrt{2}$ tales que

$$C_1 \subset F \subset C_2.$$

Por lo tanto, $\pi(\sqrt{n}-\sqrt{2})^2 \leq R(n) \leq \pi(\sqrt{n}+\sqrt{2})^2$, lo cual implica que $R(n) = \pi n + O(\sqrt{n})$. □

Este resultado fue obtenido por Gauss a principios del siglo pasado. En torno al año 1906, W. Sierpinski demostró que el error $E(n) = |R(n) - \pi n|$ era $O(n^{1/3})$. El mejor resultado hasta la fecha se debe a Iwaniec: $E(n) = O(n^{\frac{7}{22}+\epsilon})$ para todo $\epsilon > 0$.

En el otro sentido Hardy y Landau probaron que la relación $E(n) = O(n^{1/4})$ es falsa. Es un famoso problema de la teoría de los números encontrar el orden de magnitud exacto del error $E(n)$. ¿Es cierto que $E(n) = O(n^{1/4+\epsilon})$ para todo $\epsilon > 0$?

2.1.10. Promedio de la función divisor

La función $d(n)$ ha sido estudiada en el capítulo anterior. Análogamente al caso anterior, consideramos,

$$D(n) = \sum_{k=1}^{n} d(k).$$

EL cociente $\frac{D(n)}{n}$ mide el número de divisores que, en promedio, tiene un número comprendido entre 1 y n.

Veamos la interpretación geométrica: $d(n)$ es el número de puntos de coordenadas enteras del primer cuadrante que están sobre la hipérbola $xy = n$ y $D(n)$ es el número de puntos que se encuentran en la región R comprendida entre la hipérbola $xy = n$ y las rectas $x = 1$, $y = 1$.

Teorema 2.1.19.

$$D(n) = n\log n + (2\gamma - 1)n + O(\sqrt{n})$$

donde γ es la constante de Euler.

Demostración.

$$\begin{aligned} D(n) &= \sum_{k\leq n} d(k) = \sum_{k\leq n}\sum_{ab=k} 1 = \sum_{ab\leq n} 1 \\ &= \sum_{\substack{ab\leq n \\ a\leq\sqrt{n}}} 1 + \sum_{\substack{ab\leq n \\ b\leq\sqrt{n}}} 1 - \sum_{\substack{ab\leq n \\ a,b\leq\sqrt{n}}} 1 = 2\sum_{\substack{ab\leq n \\ a\leq\sqrt{n}}} -[\sqrt{n}]^2 \\ &= 2\sum_{a\leq\sqrt{n}} \left\lfloor \frac{n}{a} \right\rfloor - n + O(\sqrt{n}) = 2\sum_{a\leq\sqrt{n}} \frac{n}{a} - n + O(\sqrt{n}) \\ &= 2n\log(\sqrt{n}) + 2n\gamma - n + O(\sqrt{n}). \end{aligned}$$

□

2.1.11. Puntos visibles desde el origen

Un punto de coordenadas enteras es visible desde el origen si el segmento rectilíneo que une dicho punto con el origen no contiene a ningún otro.

Es fácil observar que el punto de coordenadas enteras (a, b) es visible desde el origen si y sólo si $(a, b) = 1$.

Consideremos la región cuadrada del plano $1 \leq x \leq r,\ 1 \leq y \leq r$.

Sea $N(r)$ el número de puntos de coordenadas enteras en este cuadrado y sea $N'(r)$ el número de ellos que son visibles desde el origen.

El cociente $\frac{N'(r)}{N(r)}$ mide la proporción de puntos del cuadrado que son visibles desde el origen.

Teorema 2.1.20. *El conjunto de coordenadas enteras visibles desde el origen tiene densidad* $\frac{6}{\pi^2}$.

Demostración. Por simetría tenemos que

$$N'(r) = -1 + 2 \sum_{1 \leq n \leq r} \sum_{\substack{1 \leq m \leq n \\ (m,n)=1}} 1 = -1 + 2 \sum_{1 \leq n \leq r} \phi(r)$$

donde ϕ es la función de Euler.

Recordando que $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$ y reordenando las sumas tenemos

$$\begin{aligned}
\sum_{n \leq r} \phi(n) &= \sum_{n \leq r} \sum_{d|n} \mu(d) \frac{n}{d} = \sum_{n \leq r} \sum_{\substack{q,d \\ qd=r}} \mu(d) q \\
&= \sum_{\substack{q,d \\ qd \leq r}} \mu(d) q = \sum_{d \leq r} \mu(d) \sum_{q \leq [r/d]} q = \sum_{d \leq r} \mu(d) \left\{ \frac{[r/d]([r/d]+1)}{2} \right\} \\
&= \sum_{d \leq r} \mu(d) \left\{ \frac{r^2}{d^2} + O(\frac{r}{d}) \right\} = \frac{r^2}{2} \sum_{d \leq r} \frac{\mu(d)}{d^2} + O\left(r \sum_{d \leq r} \frac{1}{d} \right) \\
&= \frac{r^2}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - \frac{r^2}{2} \sum_{d > r} \frac{\mu(d)}{d^2} + O\left(r \sum_{d \leq r} \frac{1}{d} \right) = \frac{r^2}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(r \log r).
\end{aligned}$$

Para calcular la constante $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}$ volvamos a la identidad de Euler comentada en el capítulo 1.

Si $s > 1$ teníamos que $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$. Entonces

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Es bien conocido que $\zeta(2) = \frac{\pi^2}{6}$. Asumiendo este hecho, tenemos que

$$\sum_{n \leq r} \phi(n) = \frac{3}{\pi^2} r^2 + O(r \log r).$$

Obviamente $N(r) = r^2 + O(r)$. Luego

$$\frac{N'(r)}{N(r)} = \frac{\frac{6}{\pi^2} r^2 + O(r \log r)}{r^2 + O(r)} = \frac{\frac{6}{\pi^2} + O\left(\frac{\log r}{r}\right)}{1 + O\left(\frac{1}{r}\right)}.$$

Haciendo tender r a infinito obtenemos el teorema.

□

2.2. Ejercicios del capítulo 2

2.2.1. *El conserje de un hotel cierra todas las puertas el primer día, el segundo abre las pares, el tercer día vuelve (si estaba abierta la cierra y viceversa) las múltiplos de* 3*, el cuarto día las múltiplos de* 4*, etcétera.*

¿Qué puertas quedarán cerradas al final del proceso?

2.2.2. *Demostrar que la función* $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$ *es multiplicativa pero no completamente multiplicativa.*

2.2.3. *Caracterizar los números que tienen* 60 *divisores.*

2.2.4. *Demostrar que* n *es perfecto si y sólo si* $\sum_{d|n} \frac{1}{d} = 2$.

2.2.5. *Determinar los enteros* n *tales que* $\prod_{d|n} d = n^2$.

2.2.6. *Demostrar que* $\sum_{m|n} d(m^2) = d^2(n)$.

2.2.7. *Demostrar que*

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^2} = \frac{\pi^4}{36}.$$

2.2.8. *Demostrar que, dado $k \geq 1$, la suma de los inversos de los enteros positivos con exactamente k divisores es convergente si y sólo si k es impar.*

2.2.9. *Demostrar las identidades*

$$\prod_{d|n} d = n^{d(n)/2}, \qquad \sum_{m|n} d^3(m) = \left(\sum_{m|n} d(m) \right)^2.$$

2.2.10. *Demostrar que un número perfecto impar no puede ser de la forma $p^\alpha q^\beta$, p, q primos. Demostrar que tampoco de la forma $p^\alpha q^\beta r^\gamma$, p, q, r primos.*

2.2.11. *Demostrar que para todo $\epsilon > 0$ se tiene $d(n) = O(n^\epsilon)$. Demostrar también que la estimación $d(n) = (\log n)^r$ no es cierta para ningún r.*

2.2.12. *Demostrar que*

$$\sum_{\substack{m \leq n \\ (m,n)=1}} m = \frac{n\phi(n)}{2}.$$

2.2.13. *Calcular* $\limsup_{n\to\infty} \frac{\phi(n)}{n}$ *y* $\liminf_{n\to\infty} \frac{\phi(n)}{n}$.

2.2.14. *Demostrar que el conjunto* $\left\{ \frac{\phi(n)}{n},\ n \geq 1 \right\}$ *es denso en el intervalo* $[0, 1]$.

2.2.15. *Demostrar que $\sigma(n) = O(n \log n)$.*

2.2.16. *Demostrar que*

$$\frac{1}{2} < \frac{\sigma(n)\phi(n)}{n^2} \leq 1.$$

2.2.17. *Usar los dos ejercicios anteriores para concluir que $\phi(n) \gg n/\log n$.*

2.2.18. *Buscar todos los enteros tales que a) $\phi(n) = \frac{n}{2}$, b) $\phi(n) = \phi(2n)$, c) $\phi(n) = 12$.*

2.2.19. *Demostrar que $\sum_{d^2|n} \mu(d) = |\mu(n)|$.*

2.2.20. *Sea $g(n) = \sum_{d|n} f(d)$. Demostrar que $f(n) = \sum_{d|n} \mu(d) g(n/d)$.*

2.2.21. *La función de Mandgoldt se define de la siguiente manera:*

$$\Lambda(n) = \begin{cases} \log p, & \text{si } n \text{ es una potencia de un primo } p \\ 0 & \text{en otro caso.} \end{cases}$$

Demostrar que $\sum_{d|n} \Lambda(d) = \log n$ y que $\sum_{d|n} \mu(d) \log d = -\Lambda(n)$.

Demostrar también que

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

2.2.22. *Demostrar que para cada* $0 \leq \alpha < 1$ *se tiene el desarrollo asintótico*

$$\sum_{n \leq x} \frac{1}{n^\alpha} = \frac{x^{1-\alpha}}{1-\alpha} + c_\alpha + O(x^{-\alpha})$$

para una constante c_α.

2.2.23. *Estimar el número de fracciones irreducibles en el intervalo* $[0, 1]$ *con denominador menor o igual que* N.

2.2.24. *Sea* $r_3(n) = \#\{n = x^2+y^2+z^2 : \ x, y, z \in \mathbb{Z}\}$. *Hallar una fórmula asintótica para* $R_3(x) = \sum_{n \leq x} r_3(n)$.

2.2.25. *Se dice que un entero positivo es libre de cuadrados si no es divisible por ningún cuadrado mayor que* 1. *Utilizar el ejercicio anterior para estimar el número de enteros positivos menores que* x *que son libres de cuadrados.*

2.2.26. *Hallar una fórmula asintótica para* $\sum_{n \leq x} \sigma(n)$ *donde* $\sigma(n) = \sum_{d|n} d$.

Capítulo 3

Congruencias

3.1. Clases residuales

En su obra Disquisitiones Arithmeticae, publicada en el año 1801, Gauss introdujo en las Matemáticas el concepto de congruencia.

Supongamos que a, b y $m > 0$ son números enteros. Diremos que a y b son congruentes módulo m si $m \mid a-b$ y designaremos esta situación mediante el símbolo $a \equiv b \pmod{m}$.

La congruencia es una relación de equivalencia puesto que verifica las propiedades reflexiva, simétrica y transitiva. Por lo tanto podemos agrupar a los enteros en familias disjuntas de manera que dos números son congruentes módulo m si y sólo si están en la misma. Estas familias se denominan clases residuales módulo m, y se designa por $\mathbb{Z}_m$ al conjunto formado por ellas.

De la definición anterior se deducen inmediatamente las siguientes propiedades.

Proposición 3.1.1. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces*

i) $a + b \equiv c + d \pmod{m}$.

ii) $ka \equiv kb \pmod{m}$ *para todo entero* $k \in \mathbb{Z}$.

iii) $ac \equiv bd \pmod{m}$.

iv) $a^n \equiv b^n \pmod{m}$

v) $f(a) \equiv f(b) \pmod{m}$ *para todo polinomio* f *con coeficientes enteros.*

Los enteros $0, 1, \ldots, m-1$ están en clases residuales distintas. Como todo entero n puede escribirse de manera única de la forma $n = mc+r$ con $0 \leq r \leq m-1$, resulta

que todo entero es congruente módulo m con uno de los enteros $0, 1, \ldots, m-1$. En particular existen exactamente m clases residuales módulo m y cualquier conjunto de enteros incongruentes módulo m constituyen un sistema residual completo.

El conjunto $\mathbb{Z}_m,\ m \geq 2$, dotado de las operaciones suma y producto emanadas de la proposición anterior es un anillo conmutativo cuyo elemento neutro aditivo, clase 0, es $0 = (m) = m\mathbb{Z}$ y cuya unidad multiplicativa es $1 + (m)$.

Proposición 3.1.2. *Si $\{a_1, \ldots, a_m\}$ es un sistema residual completo y $(k, m) = 1$, entonces el conjunto $\{ka_1, \ldots, ka_m\}$ también es un sistema residual completo.*

Demostración. Si $ka_i \equiv ka_j \pmod{m}$ entonces $m \mid k(a_i - a_j)$. Pero al ser k y m primos entre sí, $m \mid (a_i - a_j)$. Es decir, los ka_i son incongruentes entre sí módulo m y por lo tanto forman un sistema residual completo. □

De una manera análoga podemos definir un sistema residual reducido como todo conjunto de $\phi(m)$ residuos incongruentes módulo m, cada uno de ellos primo con m. De manera similar se demuestra la siguiente proposición.

Proposición 3.1.3. *Si $\{a_1, \ldots, a_{\phi(m)}\}$ es un sistema residual reducido y $(k, m) = 1$, entonces el conjunto $\{ka_1, \ldots, ka_m\}$ también es un sistema residual reducido.*

Se designa por $\mathbb{Z}_m^*$ al conjunto de las clases residuales primas con m. Es fácil ver que constituyen un grupo multiplicativo de orden $\phi(m)$.

3.2. Congruencias lineales

En esta sección intentaremos resolver la ecuación en congruencias más sencilla de todas: la congruencia lineal.

Teorema 3.2.1. *Si $(a, m) = 1$, la congruencia $ax \equiv b \pmod{m}$ tiene exactamente una solución módulo m.*

Demostración. Por la proposición 3.1.2, el conjunto $\{a, 2a, \ldots, ma\}$ es un sistema residual completo. En particular uno y sólo uno de los residuos será congruente con b módulo m. □

Lema 3.2.2. *Si $ac \equiv bc \pmod{m}$ y $d = (m, c)$, entonces $a \equiv b \pmod{m/d}$.*

Demostración. Como $m \mid c(b - a)$, entonces $(m/d) \mid (c/d)(a - b)$. Pero como $(m/d, c/d) = 1$, entonces $(m/d) \mid a - b$. □

Teorema 3.2.3. *Supongamos que* $(a, m) = d$. *Si* $d \nmid b$ *la congruencia*

$$ax \equiv b \pmod{m}$$

no tiene soluciones, mientras que si $d \mid b$ *la congruencia tiene exactamente* d *soluciones módulo* m *que vienen dadas por*

$$x_1, x_1 + m_1, \ldots, x_1 + (d-1)m_1,$$

donde x_1 *es la solución de la congruencia* $a_1 x \equiv b_1 \pmod{m_1}$ *y* $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$.

Demostración. Si la congruencia tiene alguna solución entonces, como $d \mid a$ y $d \mid b$, necesariamente tendría que dividir a b.

Cualquier solución x de $ax \equiv b \pmod{b}$ debe serlo también de $a_1 x \equiv b_1 \pmod{m_1}$. Pero como $(a_1, m_1) = 1$ la solución x_1 es única módulo m_1. Sin embargo la clase residual módulo m_1 a la que pertenece x_1 consta de d clases residuales distintas módulo m, es decir, las clases a las que pertenecen los números $x_1, x_1 + m_1, \ldots, x_1 + (d-1)m_1$. Por lo tanto la congruencia $ax \equiv b \pmod{m}$ tiene exactamente d soluciones distintas. □

Hemos visto que las congruencias lineales se reducen a resolver congruencias donde el módulo y el coeficiente de la x son primos entre sí.

La manera más económica de resolver esta ecuación consiste en resolver primero la ecuación $ax \equiv 1 \pmod{m}$ utilizando el algoritmo de Euclides y multiplicar dicha solución por b.

Ejemplo: Resolver la ecuación $51x \equiv 27 \pmod{123}$.

Observemos primero que $(51, 123) = 3$ y que 3 divide a 27. Luego esta congruencia tendrá exactamente 3 soluciones que serán $x_1, x_1 + 41, x_1 + 82$ donde x_1 es la solución de la congruencia $17x \equiv 9 \pmod{41}$. Para resolver esta congruencia resolvemos primero la congruencia $17x \equiv 1 \pmod{41}$ con el algoritmo de Euclides:

$$\begin{aligned} 41 &= 2 \cdot 17 + 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \end{aligned}$$

Yendo hacia atrás tenemos que $1 = 7 - 2 \cdot 3 = 7 - 2(17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17 = 5(41 - 2 \cdot 17) - 2 \cdot 17 = 5 \cdot 41 - 12 \cdot 17$. Es decir, $17 \cdot (-12) \equiv 1 \pmod{41}$ y por lo tanto $17 \cdot (-12 \cdot 9) \equiv 9 \pmod{41}$.

Luego $x_1 \equiv -108 \equiv 15 \pmod{41}$, y las tres soluciones de la congruencia original son $15, 56$ y 97.

Teorema 3.2.4 (Euler-Fermat)**.** *Si* $(a, m) = 1$*, entonces* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración. Sea $r_1, \ldots, r_{\phi(m)}$ un sistema residual reducido módulo m. Entonces, por la proposición 3.1.3, $ar_1, \cdots, ar_{\phi(m)}$ es también un sistema residual reducido módulo m. Los productos de todos los elementos en cada sistema tienen que coincidir módulo m,

$$r_1 \cdots r_{\phi(m)} \equiv a^{\phi(m)} r_1 \cdots r_{\phi(m)} \pmod{m}$$

y como $r_1 \cdots r_{\phi(m)}$ es primo con m, podemos cancelarlo (ver lema 3.2.2) para obtener $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Teorema 3.2.5 (Fermat)**.** *Para todo primo* p *y para todo entero* a *tal que* $(a, p) = 1$*, se verifica la congruencia* $a^{p-1} \equiv 1 \pmod{p}$.

Demostración. Basta con observar que $\phi(p) = p - 1$. □

El teorema de Euler-Fermat nos proporciona una solución explícita de la congruencia $ax \equiv b \pmod{m}$ cuando $(a, m) = 1$. Esta es $x = ba^{\phi(m)-1}$.

En el ejemplo anterior tendríamos que $x_1 \equiv 9 \cdot 17^{39} \pmod{41}$. Para calcular $17^{39} \pmod{41}$ calculamos

$$\begin{aligned}
17^{2^0} &\equiv 17 \pmod{41} \\
17^{2^1} &\equiv 2 \pmod{41} \\
17^{2^2} &\equiv 4 \pmod{41} \\
17^{2^3} &\equiv 16 \pmod{41} \\
17^{2^4} &\equiv 10 \pmod{41} \\
17^{2^5} &\equiv 18 \pmod{41}
\end{aligned}$$

y como $39 = 2^5 + 2^2 + 2^1 + 2^0$ entonces $17^{39} \equiv 18 \cdot 4 \cdot 2 \cdot 17 \equiv 29 \pmod{41}$. Luego $x_1 \equiv 29 \cdot 9 \equiv 15 \pmod{41}$ y a partir de aquí se procede como antes.

3.3. Congruencias polinómicas. Teorema de Lagrange

El estudio de congruencias polinómicas de grado superior resulta más complicado. Únicamente para las congruencias de grado 2 existe un método razonable (que se verá en el siguiente capítulo) para decidir cuándo tienen solución.

Cuando el módulo es primo tenemos, sin embargo, el siguiente teorema.

Teorema 3.3.1 (Lagrange)**.** *Dado un primo p, sea $f(x) = c_0 + c_1x + \cdots + c_nx^n$ un polinomio de grado n con coeficientes enteros tal que $p \nmid c_n$. Entonces la congruencia polinómica $f(x) \equiv 0 \pmod{p}$ tiene, a lo más, n soluciones.*

Demostración. Vamos a proceder por inducción sobre el grado del polinomio.

El caso $n = 1$ ha sido estudiado anteriormente. La congruencia $c_0 + c_1x \equiv 0 \pmod{p}$ tiene una solución si $(c_1, p) = 1$.

Hagamos la hipótesis de que el teorema es cierto para $n-1$: si x_1 es una solución de $c_0 + \cdots + c_nx^n \equiv 0 \pmod{p}$, la ecuación $c_1(x - x_1) + \cdots + c_n(x^n - x_1^n) \equiv 0 \pmod{p}$ debe ser verificada por cualquier otra solución.

Es decir, existen enteros $a_2, a_3, \ldots, a_n$ tales que

$$(x - x_1)(c_nx^{n-1} + a_2x^{n-2} + \cdots + a_n) \equiv 0 \pmod{p}$$

debe ser satisfecha por todas las soluciones de nuestra ecuación.

Como p es primo, las soluciones distintas de x_1 deben serlo también de $c_nx^{n-1} + a_2x^{n-2} + \cdots + a_n \equiv 0 \pmod{p}$ y, por hipótesis de inducción, existen, a lo sumo, $n - 1$ soluciones de esta ecuación, lo cual completa la demostración del teorema de Lagrange. □

Corolario 3.3.2. *Si la congruencia*

$$c_nx^n + c_{n-1}x^{n-1} + \cdots + c_0 \equiv 0 \pmod{p}$$

tiene más de n soluciones, entonces los coeficientes $c_0, c_1, \ldots, c_n$ deben ser múltiplos de p.

Demostración. Supongamos que no es cierto y sea r el mayor entero tal que $p \nmid c_r$. La congruencia del corolario es equivalente a la congruencia $c_rx^r + \cdots + c_0 \equiv 0 \pmod{p}$, que tiene a lo más r soluciones. La contradicción surge porque estamos suponiendo que tiene por lo menos $n + 1$ soluciones. □

En particular consideremos la congruencia

$$(x - 1)(x - 2)\cdots(x - (p - 1)) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

El grado de esta congruencia es $p-2$ y, sin embargo, tiene $p-1$ soluciones por el teorema de Euler-Fermat. Por lo tanto, todos los coeficientes deben ser múltiplos de p.

Teorema 3.3.3 (Wilson)**.**

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Demostración. Aplicar la observación anterior al término independiente. □

Observación: Toda congruencia de la forma

$$a_n x^n + \cdots + a_0 \equiv 0 \pmod{p}$$

es equivalente a una de grado menor o igual que $p-1$. Para verlo basta con aplicar el teorema de Fermat $x^p \equiv x \pmod{p}$.

3.4. Congruencias simultaneas. Teorema Chino del resto

A continuación vamos a cambiar de tercio y en vez de una sola congruencia vamos a considerar sistemas de ellas.

Consideremos el sistema

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \cdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

donde $(m_i, m_j) = 1,\ i \neq j$.

Definamos $m = m_1 m_2 \cdots m_k = m_1 M_1 = \cdots = m_k M_k$.

Como $(m_j, M_j) = 1$ sabemos que existe una solución única, módulo m_j de la ecuación $M_j x \equiv 1 \pmod{m_j}$. Sea M_j' dicha solución y consideremos el número

$$x' = M_1 M_1' b_1 + \cdots + M_k M_k' b_k.$$

Es claro que $x' \equiv M_j M_j' b_j \equiv b_j \pmod{m_j}$ para todo j, ya que M_i' es un múltiplo de m_j para $i \neq j$ y $M_j M_j' \equiv 1 \pmod{b_j}$.

Por otra parte, si x es otra solución del sistema entonces $x \equiv x' \pmod{m_j}$ para todo j y, como los números $m_1, \ldots, m_k$ son primos entre sí, resulta que $x \equiv x' \pmod{m}$.

Hemos demostrado entonces el siguiente teorema:

Teorema 3.4.1 (Chino del resto)**.** *Si los números $m_1, \ldots, m_k$ son primos entre sí, entonces el sistema*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \cdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

tiene una única solución módulo m y ésta viene dada por

$$x' = M_1 M_1' b_1 + \cdots + M_k M_k' b_k.$$

Veamos ahora una aplicación del teorema chino del resto a congruencias polinómicas respecto a un módulo compuesto.

Supongamos que los números $m_1, \ldots, m_k$ son primos entre sí dos a dos y consideramos la congruencia

$$a_n x^n + \cdots + a_0 \equiv 0 \pmod{m}.$$

Esta ecuación es equivalente al sistema

$$\begin{cases} a_n x^n + \cdots + a_0 \equiv 0 \pmod{m_1} \\ \cdots \\ \cdots \\ a_n x^n + \cdots + a_0 \equiv 0 \pmod{m_1} \end{cases}$$

Teorema 3.4.2. *El número de raíces de la ecuación es el producto de raíces de cada una de las congruencias que aparecen en el sistema.*

Demostración. En primer lugar es claro que cada solución de la ecuación satisface el sistema.

Por otro lado, si $r_1, \ldots, r_k$ es un sistema de soluciones del sistema y si x es la solución de

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ \cdots \\ \cdots \\ x \equiv r_k \pmod{m_k} \end{cases}$$

dada por la proposición anterior, entonces

$$a_n x^n + \cdots + a_0 \equiv a_n r_j^n + \cdots + a_0 \equiv 0 \pmod{m_j}$$

para todo j y, por tanto,

$$a_n x^n + \cdots + a_0 \equiv 0 \pmod{m_1 \cdots m_k}.$$

□

EJEMPLO: Para resolver $x^3 + 2x - 3 \equiv 0 \pmod{15}$ escribimos el sistema

$$\begin{cases} x^3 + 2x - 3 \equiv 0 \pmod{3} \\ x^3 + 2x - 3 \equiv 0 \pmod{5} \end{cases}.$$

La primera de estas ecuaciones tiene soluciones $x = 0, 1, 2$ módulo 3 y la segunda $x = 1, 3, 4$ módulo 5.

Por lo tanto, la ecuación $x^3 + 2x - 3 \equiv 0 \pmod{15}$ tiene 9 soluciones. Para encontrarlas teneos que resolver los 9 sistemas

$$\begin{cases} x \equiv a \pmod{3} \\ x \equiv b \pmod{5} \end{cases} \qquad a = 0, 1, 2 \qquad b = 1, 3, 4.$$

Por lo visto en los ejemplos anteriores, el problema de encontrar las soluciones de

$$P(x) = a_n x^n + \cdots + a_0 \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}$$

queda reducido a estudiar congruencias de la forma $P(x) \equiv 0 \pmod{p^\alpha}$, donde p es un número primo.

A continuación vamos a presentar una estrategia que nos permite reducir dicho estudio al caso sencillo $\alpha = 1$.

Si

$$f(a) \equiv 0 \pmod{p^\alpha}, \qquad 0 \leq a < p^\alpha,$$

entonces $f(a) \equiv 0 \pmod{p^{\alpha-1}}$ y a será de la forma $a = qp^{\alpha-1} + r$ con $0 \leq r < p^{\alpha-1}$ para algún q, $0 \leq q < p$.

Claramente $f(a) \equiv f(r) \equiv 0 \pmod{p^{\alpha-1}}$ y decimos que r ha sido generado por a.

Es decir, cada solución de $f(x) \equiv 0 \pmod{p^\alpha}$ genera otra de $f(x) \equiv 0 \pmod{p^{\alpha-1}}$.

Pero precisamente estamos buscando el proceso contrario. Si $f(r) \equiv 0 \pmod{p^{\alpha-1}}$, ¿cuándo existe un a tal que $f(a) \equiv 0 \pmod{p^\alpha}$ y que genere r? Cuando esto ocurra diremos que r puede subirse de $p^{\alpha-1}$ a p^α.

Teorema 3.4.3. *Sea $\alpha \geq 2$ y r una solución de*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}, \quad 0 \leq r < p^{\alpha-1}.$$

a) Si $f'(r) \not\equiv 0 \pmod{p}$, entonces r se sube de manera única de $p^{\alpha-1}$ a p^α.

b) $f'(r) \equiv 0 \pmod{p}$

b_1) *Si* $f(r) \equiv 0 \pmod{p^\alpha}$, *entonces* r *puede subirse de* $p^{\alpha-1}$ *a* p^α *de* p *formas diferentes.*

b_2) *Si* $f(r) \not\equiv 0 \pmod{p^\alpha}$, *entonces* r *no puede subirse de* $p^{\alpha-1}$ *a* p^α.

Demostración. Si a genera r, a tiene que ser de la forma

$$a = r + qp^{\alpha-1}, \quad 0 \leq r < p^{\alpha-1}, \quad 0 \leq q < p$$

y además $f(a) \equiv 0 \pmod{p^\alpha}$.

Por lo fórmula de Taylor en el punto r tenemos

$$f(r + qp^{\alpha-1}) = f(r) + qp^{\alpha-1}f'(r) + (qp^{\alpha-1})^2\frac{f''(r)}{2} + \cdots$$

Observemos que todos los sumandos a partir del tercero son múltiplos de p^α. Luego

$$0 \equiv f(r + qp^{\alpha-1}) \equiv f(r) + qp^{\alpha-1}f'(r) \pmod{p^\alpha}.$$

Como $f(r) = kp^{\alpha-1}$ para algún entero k, deberemos encontrar q tal que

$$k + qf'(r) \equiv 0 \pmod{p}.$$

Si $f'(r) \not\equiv 0 \pmod{p}$ dicho q existe y es único y por tanto r puede subirse de manera única.

Si $f'(r) \equiv 0 \pmod{p}$ y $f(r) \equiv 0 \pmod{p^\alpha}$ entonces $p \mid k$ y $k + qf'(r) \equiv 0 \pmod{p}$ para todo $q,\ 0 \leq q < p$. Es decir, r se puede subir de p maneras diferentes.

Si $f'(r) \equiv 0 \pmod{p}$ y $f(r) \not\equiv 0 \pmod{p^\alpha}$ entonces $p \nmid k$ y r no se puede subir porque no existe ningún q tal que $k + qf'(r) \equiv 0 \pmod{p}$. □

3.5. Raíces primitivas

Supomgamos que $(a, m) = 1$. El teorema de Euler nos asegura que $a^{\phi(m)} \equiv 1 \pmod{m}$, pero es posible que $\phi(m)$ no sea necesariamente el entero positivo más pequeño que verifica la ecuación $a^x \equiv 1 \pmod{m}$.

Definicion 3.5.1. *Dados dos números primos entre sí,* a *y* m, *llamaremos exponente de* a *módulo* m *al menor entero positivo* e *tal que* $a^e \equiv 1 \pmod{m}$. *Usaremos la notación* $e = \exp_m(a)$.

Claramente si $a \equiv b \pmod{m}$ se verifica que $\exp_m(a) = \exp_m(b)$. Esto nos permite considerar, indistintamente, exponentes de enteros o de clases residuales primas módulo m.

Teorema 3.5.2. *Si $e = exp_m(a)$ entonces los números $a^0, a^1, \ldots a^{e-1}$ son incongruentes entre sí módulo m.*

Además $a^k \equiv a^j \pmod{m}$ si y sólo si $k \equiv j \pmod{e}$; en particular $a^k \equiv 1 \pmod{m}$ si y sólo si k es divisible por e.

Demostración. Sean $k = c_1 e + r_1,\ j = c_2 e + r_2,\ 0 \leq r_1 \leq r_2 < e$ y supongamos que $a^k \equiv a^j \pmod{m}$. Entonces $a^{r_1} \equiv a^{r_2} \pmod{m}$, lo que implica que $a^{r_2 - r_1} \equiv 1 \pmod{m}$ y, por tanto, $r_1 = r_2$ debido a la propia definición del exponente e. □

Los números $\exp_m(a)$ son, por tanto, divisores del número $\phi(m)$.

Puede darse el caso de que exista g de manera que $\exp_m(g) = \phi(m)$. Es este un caso importante que recibe un nombre especial, se dice que g es una raíz primitiva módulo m.

La existencia de una raíz primitiva g es equivalente a que el grupo multiplicativo $\mathbb{Z}_m^*$ sea cíclico y generado por las potencias de g.

A continuación vamos a caracterizar los módulos m para los que existen raíces primitivas.

Teorema 3.5.3. *Existen raíces primitivas módulo m si y sólo si $m = 1, 2, 4, p^k, 2p^k$, donde p designa a un número primo impar.*

Demostración. Veremos primero que si m es de la forma $1, 2, 4, p^k$ o $2p^k$ con p primo impar, entonces $\mathbb{Z}_m^*$ es cíclico. Lo haremos en varios pasos:

(1) Los casos $m = 1, 2$ son triviales. $\mathbb{Z}_4^* = \{1, 3\}$ y es claro que 3 es una raíz primitiva.

(2) Consideremos ahora $\mathbb{Z}_p^*$ con p primo impar.

Sea $f(d) = \#\{a \in \mathbb{Z}_p^* :\ \exp_m(a) = d\}$, donde d es un divisor de $\phi(p) = p - 1$. Es claro que $\sum_{d|p-1} f(d) = p - 1$.

Por otro lado sabemos que $\sum_{d|p-1} \phi(d) = p - 1$. Si probamos la desigualdad $f(d) \leq \phi(d)$ para todo $d \mid p - 1$, las dos identidades anteriores fuerzan la igualdad $f(d) = \phi(d)$ para todo divisor de $p - 1$. En particular $f(p - 1) = \phi(p - 1)$. Es decir, existen $\phi(p - 1)$ raíces primitivas módulo p.

Para completar el argumento sólo nos queda demostrar la desigualdad $f(d) \leq \phi(d)$:

Dado $d \mid p - 1$, si $f(d) \neq 0$ necesariamente existe un elemento $a \in \mathbb{Z}_p^*$ tal que $d = \exp_p(a)$ y, en particular, $a^d \equiv 1 \pmod{p}$.

La congruencia $x^d \equiv 1 \pmod{p}$ admite, a lo más, d soluciones módulo p y como la colección $1, a, \ldots, a^{d-1}$ la satisface y son, además, incongruentes entre sí módulo p, constituyen un conjunto completo de soluciones.

Sólo nos queda contar cuántas de entre ellas tienen exponente igual a d. Es claro que $\exp_p(a^k) = d$ si y sólo si $(k, d) = 1$ y, por tanto, su cardinal es $\phi(d)$ como queríamos demostrar.

(3) Sea g una raíz primitiva módulo p. Es claro que $g + tp$ es también una raíz primitiva módulo p cualquiera que sea el entero t.

Consideremos

$$\begin{aligned}(g+tp)^{p-1} &= g^{p-1} + (p-1)g^{p-2}tp + Ap^2 \\ &= 1 + sp - g^{p-2}tp + Bp^2 \\ &= 1 + p(s - gp^{p-2}t) + Bp^2,\end{aligned}$$

donde A, s, B son enteros y $g^{p-1} = 1 + sp$.

Podemos elegir el entero t de manera que $s - g^{p-2}t \not\equiv 0 \pmod{p}$, es decir, $(g + tp)^{p-1} = 1 + pu, \quad u \equiv 0 \pmod{p}$.

Vamos a probar que, con dicha elección, $g + tp$ es una raíz primitiva módulo p^k, para todo $k \geq 1$.

Supongamos que $(g + tp)^d \equiv 1 \pmod{p^k}$, siendo d un divisor de $\phi(p^k) = p^k(p-1)$.

Como $g^d \equiv 1 \pmod{p}$ y g es una raíz primitiva módulo p, d habrá de ser un múltiplo de $p - 1$ y, por tanto, podemos suponer que tiene la forma $d = p^l(p-1),\ 0 \leq l \leq k-1$.

Ahora bien, como

$$(g+tp)^{p^l(p-1)} = (1+up)^{p^l} = 1 + u_{l+1}p^{l+1}$$

con $u_{l+1} \not\equiv 0 \pmod{p}$, necesariamente ha de ser $l = k - 1$.

(4) En el caso restante, $m = 2p^k$, p primo impar, podemos proceder de la manera siguiente:

Sea g una raíz primitiva módulo p^k. Obviamente $g + p^k$ también lo es. Sea h el elemento impar del conjunto $\{g, g + p^k\}$. Vamos a ver que h es raíz primitiva módulo $2p^k$.

Como $h^{\phi(2p^k)} \equiv h^{\phi(p^k)} \equiv 1 \pmod{p^k}$ y obviamente $h^{\phi(2p^k)} \equiv 1 \pmod{2}$, entonces $h^{\phi(2p^k)} \equiv 1 \pmod{2p^k}$.

Por otro lado, si d divide a $\phi(2p^k) = \phi(p^k)$ y es tal que $h^d \equiv 1 \pmod{2p^k}$, al ser h impar, también será cierto que $h^d \equiv 1 \pmod{p^k}$ y por tanto $g^d \equiv 1 \pmod{p^k}$. Pero como g es una raíz primitiva módulo p^k entonces $\phi(p^k) \mid d$, lo que implica que $d = \phi(2p^k)$. Luego h es una raíz primitiva.

Para concluir la demostración del teorema tenemos que probar que $\mathbb{Z}_m^*$ no es cíclico si m no es uno de los enteros considerados en los casos anteriores. Lo haremos en dos pasos.

(5) Caso $m = 2^k,\ k \geq 3$.

Es una consecuencia de la observación siguiente: Si a es un número impar, entonces $a^{\frac{\phi(2^n)}{2}} \equiv 1 \pmod{2^k}$.

Lo demostraremos por inducción en k. El caso $k = 3$ se comprueba directamente. Observemos que $\frac{\phi(2^3)}{2} = 2$ y que $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{2^3}$.

Supongamos el resultado cierto para k: $a^{\frac{\phi(2^k)}{2}} = 1 + 2^k n$. Elevando ambos miembros al cuadrado obtenemos

$$a^{\phi(2^k)} = 1 + (n + n^2 2^{k-1})2^{k+1} \equiv 1 \pmod{2^{k+1}}.$$

Basta, pues, observar que $\phi(2^k) = 2^{k-1} = \frac{1}{2}\phi(2^{k+1})$.

(6) En el caso general $m = 2^k p_1^{a_1} \cdots p_r^{a_r}$, donde $k \geq 2$ si $r = 1$ y $r \geq 2$ si $k = 0$ o $k = 1$, también demostraremos que si $(a, m) = 1$ entonces $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{m}$.

Sea g una raíz primitiva módulo $p_1^{a_1}$, y sea n un entero positivo tal que $g^n \equiv a \pmod{p_1^{a_1}}$.

Tenemos que

$$a^{\frac{\phi(m)}{2}} \equiv g^{n\frac{\phi(m)}{2}} \equiv g^{\phi(p_1^{a_1})\frac{1}{2}n\phi(2^k)\phi(p_2^{a_2})\cdots\phi(p_r^{a_r})} \pmod{m}.$$

Es claro que bajo nuestras hipótesis sobre el número m, podemos afirmar que el exponente $\frac{1}{2}n\phi(2^k)\phi(p_2^{a_2})\cdots\phi(p_r^{a_r})$ es un entero.

En particular la congruencia anterior nos indica que

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{p_1^{a_1}}.$$

De manera análoga podemos probar que

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{p_i^{a_i}}, \qquad i = 1, \ldots, r.$$

Nos queda por probar que la congruencia anterior también se verifica para el módulo 2^k.

Si $k \geq 3$ aplicamos la misma demostración del caso (5) para obtener que

$$a^{\frac{\phi(2^k)}{2}} \equiv 1 \pmod{2^k}.$$

Y como $\frac{\phi(2^k)}{2}$ es un divisor de $\frac{\phi(m)}{2}$ habríamos acabado.

Si $k \leq 2$ tenemos que $\phi(m) = \phi(2^k)\phi(p_1^{a_1}) \cdots \phi(p_r^{a_r}) = 2n\phi(2^k)$ para algún entero n. Por tanto, también es cierto que

$$a^{\frac{\phi(m)}{2}} = a^{n\phi(2^k)} \equiv 1 \pmod{2^k},$$

como queríamos probar.

□

En el apartado (2) hemos observado que existen exactamente $\phi(p-1) = \phi(\phi(p))$ raíces primitivas módulo el primo impar p. Esto sigue siendo cierto para el caso general.

Sea g una raíz primitiva módulo m. Es claro que el conjunto

$$\{g^k : \ 1 \leq k \leq \phi(m), \ (k, \phi(m)) = 1\}$$

consiste, precisamente, de todas las raíces primitivas módulo m. Por lo tanto, si $m = 1, 2, 4, p^k$ ó $2p^k$, p primo impar, existen exactamente $\phi(\phi(m))$ raíces primitivas módulo m o, lo que es igual, el grupo cíclico $\mathbb{Z}_m^*$ tiene $\phi(\phi(m))$ generadores.

Observemos también que, fijada una raíz primitiva g módulo m, entonces $\{1, g, \ldots, g^{\phi(m)-1}\}$ es un sistema residual reducido módulo m.

Por lo tanto, dado a, primo con m, podemos asignarle un único número k, $\quad 0 \leq k \leq \phi(m) - 1$ de manera que $a \equiv g^k \pmod{m}$.

3.6. Ejercicios del capítulo 3

3.6.1. *Se ha escrito un número. Luego se ha escrito otro, permutando las cifras del primero. La diferencia de los dos números es* $391738X$ *¿Qué dígito es la última cifra representada por* X*?*

3.6.2. *Sea* S *un conjunto de* n *enteros no necesariamente distintos. Demostrar que algún subconjunto no vacío de* S *posee una suma divisible por* n*.*

3.6.3. *Demostrar que* $\sum_{k=1}^{n} k10^k$ *es múltiplo de* 3 *si y sólo si* $n \not\equiv 1 \pmod 3$.

3.6.4. *Hallar el resto al dividir el número* 999 998 997 ... 003 002 001 000 *entre* 13.

3.6.5. *El número n expresado en base* 2 *se escribe* 10010100111010100011, *Decir si es múltiplo de* 3.

3.6.6. *Probar el recíproco del teorema de Wilson: Si* $(n-1)!+1 \equiv 0 \pmod n$, *entonces n es primo.*

3.6.7. *Demostrar que si* $n+2$ *es primo,* $n>1$, *entonces* $n2^n+1$ *no es primo.*

3.6.8. *Sea la función* $f(x,y) = \frac{y-1}{2}\{|B^2-1| - (B^2-1)\}+2$ *donde* $B = x(y+1)+y!+1$.

a) Demostrar que $f(x,y)$ *es primo para todo* $x, y \in \mathbb{Z}$.

b) Demostrar que para todo primo $p \neq 2$, *existen unos únicos x e y tales que* $f(x,y) = p$.

3.6.9. *Demostrar que para todo* $n \geq 3$,

$$\pi(n) = 1 + \sum_{j=3}^{n} \left\{ (j-2)! - j\left[\frac{(j-2)!}{j}\right] \right\}.$$

3.6.10. *Sean* a, b, x_0 *enteros positivos, y sea* $x_n = ax_{n-1}+b$ *para todo* $n \geq 1$. *Demostrar que* x_n *no puede ser primo para todo n.*

3.6.11. *D. José estudió en un colegio que tenía entre* 150 *y* 300 *colegiales. Ahora, aunque no recuerda el número de colegiales que eran, sí se queja de no haber podido practicar ni fútbol, ni baloncesto, ni balonmano porque, cuando en cada deporte se intentaba organizar el colegio en equipos, siempre faltaba o sobraba uno. ¿Podrías recordar a D.José cuántos colegiales eran?*

3.6.12. *Caracterizar los enteros x que satisfacen simultaneamente las congruencias* $x \equiv 7 \pmod k$, $2 \leq k \leq 10$. *¿Puede alguno de estos enteros ser un cuadrado?*

3.6.13. *Hallar todas las soluciones de la congruencia* $x^3+2x^2-x+6 \equiv 0 \pmod{98}$.

3.6.14. *Demostrar que si* $a^h \equiv 1 \pmod n$ *para todo a,* $(a,n) = 1$, *entonces h divide a* $\phi(n)$.

3.6.15. *Demostrar que el conjunto de puntos de coordenadas visibles desde el origen contiene cuadrados vacíos tan grandes como queramos.*

3.6.16. *Demostrar que* $a^{560} \equiv 1 \pmod{561}$ *para todo* $(a, 561) = 1$.

3.6.17. *Para cada entero positivo n encontrar la última cifra de $13^{n!}$.*

3.6.18. *Demostrar que existen infinitos enteros positivos que no son suma de tres cuadrados.*

3.6.19. *Sea F_n un número de Fermat y p un primo. Demostrar que si p divide a F_n entonces $p = 2^{n+1}k + 1$ para algún entero k.*

3.6.20. *Probar que todo entero satisface alguna de las congruencias*

$$x \equiv 0 \pmod 2,\ x \equiv 3 \pmod 3,\ x \equiv 1 \pmod 4,$$

$$x \equiv 3 \pmod 8,\ x \equiv 7 \pmod{12},\ x \equiv 23 \pmod{24}.$$

3.6.21. *Sea m el menor módulo de un sistema de congruencias de módulos distintos que, como el del problema anterior, cubre todos los enteros. Hallar un sistema con $m = 3$. En el problema anterior, $m = 2$.*

Erdős conjeturó que se puede elegir m arbitrariamente grande pero nadie ha sido capaz de probarlo.

Capítulo 4

Ley de reciprocidad cuadrática

En el capítulo anterior hemos desarrollado con detalle la teoría de las congruencias lineales $ax + b \equiv c \pmod{m}$. Ahora vamos a considerar las congruencias cuadráticas $x^2 \equiv a \pmod{m}$.

4.1. Residuos cuadráticos

Definicion 4.1.1. *Dada una clase residual prima módulo m, representada por el entero a, diremos que es un residuo cuadrático si la congruencia $x^2 \equiv a \pmod{m}$ tiene solución. En caso contrario diremos que a es un residuo cuadrático.*

Es claro que el carácter cuadrático es independiente del representante elegido.

En lo sucesivo mantendremos la ambigüedad consistente en hablar de un entero particular como residuo o no residuo, en vez de mencionar a la clase residual que lo contiene.

Proposición 4.1.2. *Sea p un número primo impar. Existen exactamente $\frac{p-1}{2}$ residuos cuadráticos y $\frac{p-1}{2}$ residuos no cuadráticos módulo p.*

Demostración. Consideremos el siguiente sistema residual completo módulo p:

$$\left\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\right\}.$$

Como $(-k)^2 = k^2$, existen, a lo más, $\frac{p-1}{2}$ residuos cuadráticos.

Por otro lado, la congruencia $k^2 \equiv j^2 \pmod{p}$, $1 \leq k, j \leq \frac{p-1}{2}$, necesariamente implica la igualdad $k = j$:

$(k-j)(k+j) \equiv 0 \pmod{p}$ implica que $k-j \equiv 0 \pmod{p}$ o bien $k+j \equiv 0 \pmod{p}$, lo que junto con la relación $1 \leq k, j \leq \frac{p-1}{2}$ nos da $k = j$.

Por lo tanto, los números $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ son incongruentes entre sí módulo p. □

Definicion 4.1.3. *Dado un número primo impar p, el símbolo de Legendre* $\left(\frac{a}{p}\right)$ *es la función aritmética definida de la forma siguiente:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } a \equiv 0 \pmod{p} \\ +1, & \text{si } a \text{ es un residuo cuadrático} \\ -1, & \text{si } a \text{ no es un residuo cuadrático} \end{cases}$$

Proposición 4.1.4 (Criterio de Euler)**.** *Sea p un número impar. Tenemos que*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}, \text{ para todo entero } n.$$

Demostración. Si $n \equiv 0 \pmod{p}$, entonces el resultado es inmediato.

Supongamos que $(n, p) = 1$. El teorema de Fermat nos dice que $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Es decir, $(n^{\frac{p-1}{2}} - 1)(n^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$ y por lo tanto, una de las dos relaciones siguientes debe ser verificada:

i) $n^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$.

ii) $n^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$.

Si $\left(\frac{n}{p}\right) = 1$, la ecuación $x^2 \equiv n \pmod{p}$ tiene solución. En particular $n^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$: es decir, n verifica i): $n^{\frac{p-1}{2}} \equiv 1 = \left(\frac{n}{p}\right) \pmod{p}$.

Observemos que la ecuación $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ tiene como soluciones los $\frac{p-1}{2}$ residuos cuadráticos y que, por el teorema de Lagrange, no puede tener más soluciones.

Si $\left(\frac{n}{p}\right) = -1$, entonces n no es un residuo cuadrático y por tanto $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Necesariamente $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Corolario 4.1.5. *El símbolo de Legendre es una función completamente multiplicativa.*

Demostración.

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p}.$$

Pero como los valores que toma el símbolo de Legendre son $+1, 0, -1$, necesariamente tenemos la igualdad

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

□

4.1.1. Cálculo de los símbolos $\left(\frac{-1}{p}\right)$ y $\left(\frac{2}{p}\right)$

Proposición 4.1.6. *Sea p un número impar. Tenemos que*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4 \\ -1, & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

Demostración. Basta con aplicar el criterio de Euler y observar, como antes, que ambos miembros de la congruencia toman los valores $+1$ o -1 y, por tanto, la congruencia implica la igualdad. □

Proposición 4.1.7. *Para todo primo impar p tenemos la identidad:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}} = \begin{cases} +1, & \text{si } p \equiv \pm 1 \pmod 8 \\ -1, & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Demostración. Consideremos las $\frac{p-1}{2}$ congruencias siguientes:

$$\begin{cases} p-1 & \equiv 1(-1)^1 \pmod p \\ 2 & \equiv 2(-1)^2 \pmod p \\ p-3 & \equiv 3(-1)^3 \pmod p \\ 4 & \equiv 4(-1)^4 \pmod p \\ \cdots & \\ r & \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \pmod p \end{cases}$$

donde r es $\frac{p-1}{2}$ ó $p - \frac{p-1}{2}$ según el caso.

Multipliquemos estos sistemas de congruencias y observemos que cada entero situado en los miembros de la parte izquierda es necesariamente par. Resulta que:

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}} \pmod{p}.$$

Es decir,

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Podemos dividir por $(\frac{p-1}{2})!$ para obtener

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

que, por la misma razón de la proposición anterior, implica la igualdad:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

□

4.1.2. Ley de reciprocidad cuadrática

La ley de reciprocidad cuadrática fue descubierta por Euler en torno al año 1745. Gauss, a su vez, también la descubrió y produjo la primera demostración completa en 1796, varios años después de sus *Disquisitiones Arithmeticae*.

Hoy en día se conocen muchas demostraciones distintas. A continuación vamos a presentar una de las más sencillas conceptualmente, que está basada en el siguiente lema de Gauss.

Lema 4.1.8 (de Gauss)**.** *Sea p un primo impar y a un entero no divisible por él. Dado $x = 1, \ldots, \frac{p-1}{2}$, sea $ax \equiv \epsilon_x u_x \pmod{p}$, donde u_x es un entero del conjunto $\{1, 2, \ldots, \frac{p-1}{2}\}$ y $\epsilon_x = \pm 1$. Entonces*

$$\left(\frac{a}{p}\right) = \epsilon_1 \cdots \epsilon_{\frac{p-1}{2}}.$$

Demostración. En primer lugar observemos que dado x, $1 \leq x \leq \frac{p-1}{2}$, tanto el entero u_x, $1 \leq u_x \leq \frac{p-1}{2}$ como el número ϵ_x están unívocamente determinados por la relación

$$ax \equiv \epsilon_x u_x \pmod{p}.$$

En efecto, si $ax_1 \equiv u \pmod{p}$ y $ax_2 \equiv -u \pmod{p}$, entonces $a(x_1 + x_2) \equiv 0 \pmod{p}$, lo que es imposible por ser $1 \leq x_1, x_2 \leq \frac{p-1}{2}$.

Multiplicando las congruencias para cada $x,\ 1 \leq x \leq \frac{p-1}{2}$ obtenemos

$$a^{\frac{p-1}{2}} 1 \cdot 2 \cdots \frac{p-1}{2} \equiv \epsilon_1 \cdots \epsilon_{\frac{p-1}{2}} 1 \cdot 2 \cdots \frac{p-1}{2} \pmod{p}.$$

Es decir

$$a^{\frac{p-1}{2}} \equiv \epsilon_1 \cdots \epsilon_{\frac{p-1}{2}} \pmod{p}.$$

Basta entonces con aplicar el criterio de Euler para concluir el teorema. □

Teorema 4.1.9 (Ley de reciprocidad cuadrática)**.** *Sean p y q números primos impares distintos. Tenemos que*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Demostración. Sean $p = 2n + 1,\ q = 2m + 1$. Apliquemos el lema de Gauss para $a = q$ con respecto al conjunto $\{1, 2, \ldots, n\},\ n = \frac{p-1}{2}$.

Tenemos, para cada $x,\ 1 \leq x \leq n$,

$$qx \equiv \epsilon_x u_x \pmod{p} \text{ con } 1 \leq u_x \leq n, \qquad e_x = \pm 1.$$

Es decir, $qx = \epsilon_x u_x + py$ donde ϵ_x, u_x, y están unívocamente determinados por estas condiciones cuando x está dado.

En particular ϵ_x toma el valor -1 si y sólo si $qx = py - u_x$. O, lo que es lo mismo,

$$py = qx + u_x,\ \text{con } 1 \leq u_x \leq n.$$

Ello implica que $y > 0$ y, además,

$$y \leq \frac{1}{p}(qx + u_x) \leq \frac{1}{p}(q+1)n < \frac{q+1}{2} = m + 1.$$

En otras palabras, $e_x = -1$ si y sólo si podemos fijar un y tal que la pareja (x, y) satisface las condiciones

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ 1 \leq py - qx \leq n. \end{cases}$$

Consiguientemente, si N designa al número de tales parejas, el lema de Gauss nos da

$$\left(\frac{q}{p}\right) = (-1)^N.$$

Análogamente

$$\left(\frac{p}{q}\right) = (-1)^M,$$

donde M es el número de parejas (x, y) que verifican

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ 1 \leq qx - py \leq m. \end{cases}$$

Ahora como p y q son primos entre sí y $1 \leq x < p$ entonces $qx - py$ no puede ser nunca cero y podemos escribir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N},$$

donde ahora $M + N$ es el número de parejas que satisfacen las condiciones

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ -n \leq qx - py \leq m. \end{cases}$$

Sea S el número de parejas (x, y) tales que

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ qx - py < -n. \end{cases}$$

Sea T el número de parejas (x', y') que verifican

$$\begin{cases} 1 \leq x' \leq n \\ 1 \leq y' \leq m \\ qx' - py' > m. \end{cases}$$

Entre estos conjuntos existe una correspondencia biyectiva dada por

$$\begin{cases} x' = n + 1 - x \\ y' = m + 1 - y. \end{cases}$$

Por lo tanto $S = T$. Por otro lado $M+N+S+T = mn$, entonces $(-1)^{M+N} = (-1)^{mn}$ y el teorema queda demostrado. □

4.1.3. Ejemplos y aplicaciones

La ley de reciprocidad cuadrática es uno de los resultados más notables de la Teoría de los Números: una relación sorprendente y a la vez sencilla entre las propiedades de las congruencias $x^2 \equiv q \pmod{p}$ y $x^2 \equiv p \pmod{q}$. Es también pieza importante de otras teorías aritméticas.

a) La ley de reciprocidad cuadrática nos permite calcular el valor de $\left(\frac{m}{p}\right)$ en muchos casos.

Ejemplo 1: Supongamos que queremos estudiar si la congruencia $x^2 \equiv 315 \pmod{65537}$ tiene solución.

Por supuesto podríamos ir comprobando todos los restos módulo 65537, pero la ley de reciprocidad cuadrática nos proporciona un método mucho más rápido. Recordemos que el símbolo de Legendre es una función multiplicativa.

$$\left(\frac{315}{65537}\right) = \left(\frac{3^2 \cdot 5 \cdot 7}{65537}\right) = \left(\frac{3^2}{65537}\right)\left(\frac{5}{65537}\right)\left(\frac{7}{65537}\right)$$
$$= \left(\frac{5}{65537}\right)\left(\frac{7}{65537}\right) = (-1)^{\frac{4\cdot 65536}{4}}\left(\frac{65537}{5}\right)(-1)^{\frac{6\cdot 65536}{4}}\left(\frac{65537}{7}\right)$$
$$= \left(\frac{2}{5}\right)\left(\frac{2}{7}\right) = (-1)^{\frac{25-1}{8}}(-1)^{\frac{49-1}{8}} = -1.$$

Es decir, la congruencia $x^2 \equiv 315 \pmod{65537}$ carece de solución.

Ejemplo 2: Queremos saber si la congruencia $x^2 \equiv 236 \pmod{257}$ tiene solución.

Procedemos como en el ejemplo anterior,

$$\left(\frac{236}{257}\right) = \left(\frac{-21}{257}\right) = \left(\frac{-1}{257}\right)\left(\frac{3}{257}\right)\left(\frac{7}{257}\right)$$
$$= (-1)^{\frac{257-1}{2}}\left(\frac{257}{3}\right)(-1)^{\frac{256\cdot 2}{4}}\left(\frac{257}{7}\right)(-1)^{\frac{256\cdot 6}{4}}$$
$$= \left(\frac{2}{3}\right)\left(\frac{5}{7}\right) = (-1)(-1) = 1.$$

Luego existe solución de la congruencia $x^2 \equiv 236 \pmod{257}$. Sin embargo, la ley no nos da una pauta para encontrarla.

b) Otro ejemplo interesante de aplicaciones es el siguiente. Queremos saber para qué primos, la congruencia $x^2 \equiv 3 \pmod{p}$ tiene solución. Es decir, para

qué valores de p se tiene que $\left(\frac{3}{p}\right) = 1$.

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

Como

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv -1 \pmod 3 \end{cases}$$

y

$$(-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv -1 \pmod 4 \end{cases}$$

resulta que

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{si } p \equiv \pm 1 \pmod{12} \\ -1 & \text{si } p \equiv \pm 5 \pmod{12}. \end{cases}$$

4.2. Ejercicios del capítulo 3

4.2.1. *Demostrar que existen infinitos primos de la forma* $4n + 1$.

4.2.2. *Hallar los primos* p *para los cuales la ecuación* $x^2 \equiv 5 \pmod p$ *tiene solución.*

4.2.3. *a) Dar una condición necesaria y suficiente para que la progresión aritmética* $an + b$ *tenga infinitos cuadrados.*

b) Utilizar el apartado anterior para estudiar la existencia de infinitos cuadrados en la progresión $160 + 103n$.

4.2.4. *Dar una condición necesaria y suficiente, en función de* a, b *y* c, *para que la congruencia* $ax^2 + bx + c \equiv 0 \pmod p$ *tenga solución. Aplicar esto último para estudiar la existencia de soluciones de la congruencia* $5x^2 - 13x + 8 \equiv 0 \pmod{37}$.

4.2.5. *Caracterizar los primos para los que tiene solución la congruencia* $5x^2 - 3x + 1 \equiv 0 \pmod p$.

4.2.6. *Demostrar que para todo polinomio* $Q(x) = ax^2 + bx + c$, *no constante, existen infinitos primos para los que la congruencia* $Q(x) \equiv 0 \pmod p$ *tiene solución.*

4.2.7. *Demostrar que el producto de todos los residuos cuadráticos positivos y menores que* p *es congruente con* $(-1)^{\frac{p+1}{2}}$ *módulo* p.

4.2.8. *Demostrar que la congruencia* $x^5 \equiv 300x \pmod{101}$ *tiene una única solución.*

4.2.9. *Demostrar que la suma de tres cuadrados consecutivos no puede ser múltiplo de* 19*.*

4.2.10. *Demostrar que si* $(x, y) = 1$ *entonces* $x^2 + y^2$ *no es divisible por ningún primo* $p \equiv 3 \pmod{4}$*.*

4.2.11. *Demostrar que* n *puede escribirse como suma de dos cuadrados si y sólo si en su factorización en números primos,*

$$n = 2^{\nu} \prod_{p_j \equiv 1 \pmod 4} p_j^{\alpha_j} \prod_{q_k \equiv 3 \pmod 4} q_k^{\beta_k}$$

todos los β_k *son pares.*

4.2.12. *Considérese la congruencia* $x^2 \equiv a \pmod{p^s}$ *con* p *primo,* $s \geq 1$*,* $a = p^t b$*,* $(b, p) = 1$*. Probar que*

a) si $t \geq s$*, la congruencia tiene solución.*

b) si $t < s$*, la congruencia tiene solución si y sólo si* t *es par y* b *es un residuo cuadrático módulo* p*.*

4.2.13. *Probar que* $\sum_{x=1}^{p} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = -1$ *si* p *es cualquier primo impar.*

Capítulo 5

Ejemplos de ecuaciones diofánticas

En este capítulo estudiaremos la resolución de ecuaciones en números enteros. Son las llamadas ecuaciones diofánticas.

La ecuación $x^n + y^n = z^n,\ xyz \neq 0$ es sin lugar a dudas la más famosa de todas. Pierre de Fermat (1601-65) dijo haber demostrado que to tenía soluciones enteras para $n \geq 3$, pero que la bella demostración que había obtenido era demasiado larga para poder escribirla en los márgenes de su ejemplar del libro de Diofanto, como acostumbraba a hacer con muchas de sus observaciones. Este problema conocido como el Último Teorema de Fermat fue resuelto por Andrew Wiles en 1995. La demostración de Wiles sobrepasa con creces los propósitos de este libro, y nos conformaremos estudiando la ecuación de Fermat para los casos $n = 2, 3$ y 4.

5.1. Las ternas pitagóricas

Las ternas (x, y, z) tales que $x^2 + y^2 = z^2$ se denomina ternas pitagóricas y originan triángulos rectángulos con lados enteros.

Estudiaremos ecuaciones más generales del tipo

$$ax^2 + by^2 = cz^2,\ a, b, c \in \mathbb{Z}.$$

En general esta ecuación no tiene por qué tener soluciones, pero si encontramos una solución (x_0, y_0, z_0) vamos a poder hallar el resto por un procedimiento sencillo.

Observemos que buscar las soluciones enteras de $ax^2 + by^2 = cz^2$ es equivalente a buscar las soluciones racionales de $ax_1^2 + by_1^2 = c$, donde hemos hecho $x_1 = \frac{x}{z},\ y_1 = \frac{y}{z}$.

Es decir, habremos de encontrar los puntos (x, y) de coordenadas racionales

sobre la elipse $ax^2 + by^2 = c$.

Supongamos que mediante una simple inspección hemos encontrado un punto (x_0, y_0) de coordenadas racionales sobre la elipse. Ahora trazamos una recta que pase por dicho punto y con pendiente $r \in Q$. Esta recta cortará a la elipse en otro punto (x_0', y_0').

Si $y - y_0 = r(x - x_0)$ es la ecuación de la recta y la sustituimos en la ecuación de la elipse, $ax^2 + b(y_0 + r(x - x_0))^2 = c$ obtenemos una ecuación de segundo grado que tendrá como soluciones x_0 y x_0'.

Ahora bien, la suma de las soluciones de una ecuación de segundo grado con coeficientes racionales es racional. Por lo tanto, si x_0 era racional, x_0' debe ser racional y sustituyendo en la recta anterior tenemos que y_0' también es racional.

Por otra parte, dos puntos de coordenadas racionales sobre la elipse nos determinan una recta de pendiente racional. Es decir, existe una biyección entre las soluciones enteras de la ecuación original y los puntos x_0', y_0' obtenidos según el método anterior.

Ahora estamos en condiciones de demostrar nuestro primer teorema.

Teorema 5.1.1. *Todas las soluciones enteras de la ecuación $x^2 + y^2 = z^2$ vienen dadas por la fórmula*

$$\begin{cases} x = (n^2 - m^2)t \\ y = 2mnt \\ z = (n^2 + m^2)t \end{cases}$$

donde $t \in \mathbb{Z}$ y n, m son enteros primos entre sí y de distinta paridad.

Demostración. Empezaremos calculando las soluciones primitivas entre sí, $(x, y) = (x, z) = (y, z) = 1$.

Intentaremos hallar todas las soluciones racionales de la ecuación $x^2 + y^2 = 1$ a partir de la solución $(x_0, y_0) = (1, 0)$.

Trazaremos una recta de pendiente $\frac{n}{m}$ (fracción irreducible) que pase por el punto $(1, 0)$. Esta es la recta $y = \frac{n}{m}(x-1)$. Ahora calculamos su punto de intersección con la elipse resolviendo la ecuación

$$x^2 + \left(\frac{n}{m}(x - 1)\right)^2 = 1.$$

Así obtenemos $x_0 = 1$, la solución de la que partíamos, y $x_0' = \frac{n^2-m^2}{n^2+m^2}$.

Sustituyendo en la recta obtenemos $y_0' = -\frac{2mn}{n^2+m^2}$. Es decir,

$$\left(\frac{n^2 - m^2}{n^2 + m^2}\right)^2 + \left(\frac{2mn}{n^2 + m^2}\right)^2 = 1,$$

y por lo tanto

$$(n^2 - m^2)^2 + (2mn)^2 = (n^2 + m^2)^2.$$

Entonces $x = n^2 - m^2, \quad y = 2mn, \quad , z = m^2 + n^2$ y como estamos pidiendo que las soluciones sean primitivas, además de que $(n, m) = 1$ debe ocurrir que n y m deben de tener distinta paridad. El resto de las soluciones vienen de multiplicar x, y, z por un mismo entero t. □

5.1.1. La ecuación $x^4 + y^4 = z^2$

Aunque ya hemos señalado que la demostración del Último Teorema de Fermat es realmente difícil, hay algunos exponentes n para los que la demostración está al nivel de este libro.

Empezaremos haciéndolo para $n = 4$ utilizando para ello el llamado método del descenso, inventado por Fermat y de uso muy frecuente en la teoría de los números. De hecho demostraremos un poco más:

Teorema 5.1.2. *La ecuación $x^4+y^4 = z^2$ no tiene soluciones en enteros si $xyz \neq 0$.*

Demostración. Supongamos que nuestra ecuación tiene alguna solución. De todas las soluciones que pueda tener elijamos la solución mínima. Sea u el menor entero positivo tal que $x^4 + y^4 = u^2$ para algún x, y.

A partir de esta solución encontraremos una solución menor obteniendo así una contradicción (Método del descenso).

La ecuación $x^4 + y^4 = u^2$ se puede expresar como una terna pitagórica $(x^2)^2 + (y^2)^2 = u^2$.

Obviamente $(x, y) = 1$. Si $(x, y) = d$ tendríamos $\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{u}{d^2}\right)^2$ obteninedo una solución menor.

Por el teorema 5.1.1 tenemos

$$\begin{cases} x^2 = n^2 - m^2 \\ y^2 = 2mn \\ n = m^2 + n^2 \end{cases}$$

para algún par m, n con $(m, n) = 1$ y de distinta paridad.

Si n es par entonce $x^2 = n^2 - m^2 \equiv -1 \pmod 4$, lo cual es imposible porque -1 no es un residuo cuadrático módulo 4. Entonces n es impar y m es par. Si escribimos $m = 2m'$ tenemos que $(y/2)^2 = nm'$. Es claro que si $(n, m) = 1$ entonces

$(n, m') = 1$. Y como su producto es un cuadrado, entonces cada uno de ellos ha de ser un cuadrado: $n = b^2, \quad m' = a^2$.

Tenemos entonces que $x^2 = n^2 - m^2 = b^4 - 4a^4$. Es decir, $(2a^2)^2 + x^2 = (b^2)^2$ y nos encontramos con otra terna pitagórica. Aplicando de nuevo el teorema 5.1.1,

$$\begin{cases} 2a^2 = 2rs \\ x^2 = r^2 - s^2 \\ b^2 = r^2 + s^2 \end{cases}$$

con $(r, s) = 1$ y de distinta paridad.

De nuevo tenemos dos enteros r, s primos entre sí y cuyo producto es un cuadrado y por lo tanto lo son cada uno de ellos: $r = c^2, \quad s = d^2$.

Sustituyendo obtenemos $c^4 + d^4 = b^2$, una solución de nuestra ecuación original. Pero $b < b^4 + m^2 = u$ contradiciendo el hecho de que u era la mínima solución posible. □

5.1.2. La ecuación $x^3 + y^3 = z^3$

Antes de estudiar esta ecuación haremos algunas observaciones sobre el anillo

$$\mathbb{Z}[\omega] = \{a + b\omega : \quad a, b \in \mathbb{Z}\},$$

donde $\omega = e^{2\pi/3}$, raíz cúbica de la unidad. Las demostraciones se dejan como

1) $1 + \omega + \omega^2 = 0$ y $\overline{\omega} = \omega^2$.

2) $N(a + b\omega) = a^2 - ab + b^2$. ejercicio.

3) Las unidades de $\mathbb{Z}[\omega]$ son $\{\pm 1, \pm\omega, \pm\omega^2\}$.

4) Si $N(a + b\omega)$ es un primo en $\mathbb{Z}$, entonces $a + b\omega$ es un primo en $\mathbb{Z}[\omega]$.

5) El anillo $\mathbb{Z}[\omega]$ es un anillo euclídeo y por tanto de factorización única. Todo entero se descompone en sus factores primos de manera única excepto el orden y las unidades.

6) El entero $1 - \omega$ es primo en $\mathbb{Z}$.

La aritmética de $\mathbb{Z}[\omega]$ tiene gran interés, ya que precisamente es en $\mathbb{Z}[\omega]$ donde la ecuación $x^3 + y^3 = z^3$ se factoriza:

$$x^3 + y^3 = (x + y)(x\omega + y\omega^2)(x\omega^2 + y\omega) = z^3.$$

Teorema 5.1.3. *La ecuación $x^3+y^3=z^3,\ xyz\neq 0$ no tiene soluciones en enteros.*

Demostración. De hecho demostraremos algo más: la ecuación anterior no tiene soluciones en $\mathbb{Z}[\omega]$.

Supongamos que x, y, z son tres elementos no nulos de $\mathbb{Z}[\omega]$ tales que $x^3+y^3=z^3$. No hay nada que nos impida suponer que x, y, z son primos relativos dos a dos en $\mathbb{Z}[\omega]$. Si $d\in\mathbb{Z}[\omega]$ dividiera a dos de ellos, podríamos dividir la ecuación entre d^3 y $x/d, y/d, z/z$ sería una solución de la ecuación.

Lema 5.1.4. $a+b\omega\equiv 0, 1$ *ó* $-1 \pmod{1-\omega}$.

Demostración. Observemos que $a+b\omega\equiv a+b \pmod{1-\omega}$. Por otra parte $a+b=3q+r,\ 0\leq r<3$. Entonces,

$$a+b\omega\equiv a+b\equiv 3q+r\equiv r \pmod{1-\omega}$$

porque 3 es un múltiplo de $1-\omega$ en $\mathbb{Z}[\omega]$. □

Lema 5.1.5. *Si $\alpha\in\mathbb{Z}[\omega]$ y $\alpha\equiv\pm 1 \pmod{1-\omega}$, entonces $\alpha^3\equiv\pm 1 \pmod{(1-\omega)^4}$.*

Demostración. Como $\alpha\equiv\pm 1 \pmod{1-\omega}$ entonces $\alpha=\beta(1-\omega)\mp 1$ para algún entero $\beta\in\mathbb{Z}[\omega]$.

Elevando al cubo,

$$\alpha^3=\beta^3(1-\omega)^3\mp 3\beta^2(1-\omega)^2+3\beta(1-\omega)\mp 1.$$

Observemos ahora que $3=-\omega^2(1-\omega)^2$. Sustituyendo,

$$\begin{aligned}\alpha^3&=\beta^3(1-\omega)^3\mp -\omega^2(1-\omega)^4\beta^2-\omega^2\beta(1-\omega)^3\mp\\&=(1-\omega)^3\beta(\beta^2-\omega^2)\mp(-\omega^2\beta^2(1-\omega)^4)\mp 1.\end{aligned}$$

Para terminar la demostración debemos ver que $(1-\omega)^3\beta(\beta^2-\omega^2)\equiv 0 \pmod{(1-\omega)^4}$. Es decir, debemos ver que $\beta(\beta^2-\omega^2)\equiv 0 \pmod{1-\omega}$.

Si $\beta\equiv 0 \pmod{1-\omega}$, ya está demostrado. En otro caso, por el lema anterior, $\beta\equiv\pm 1 \pmod{1-\omega}$ y entonces $\beta^2\equiv 1 \pmod{1-\omega}$. Por tanto $\beta^2-\omega^2\equiv 0 \pmod{1-\omega}$ y el lema queda demostrado. □

Lema 5.1.6. *Si $x^3+y^3=z^3$ entonces x, y ó z tiene que ser divisible por $1-\omega$.*

Demostración. Por el lema 5.1.5, si ninguno de ellos fuese divisible por $1-\omega$ tendríamos

$$\begin{cases} x^3 \equiv \pm 1 \pmod{(1-\omega)^4} \\ y^3 \equiv \pm 1 \pmod{(1-\omega)^4} \\ z^3 \equiv \pm 1 \pmod{(1-\omega)^4}. \end{cases}$$

Entonces $(\pm 1) + (\pm 1) - (\pm 1) \equiv 0 \pmod{(1-\omega)^4}$ y los posibles valores que podríamos obtener serían $-1, 1, -3, 3$.

Pero $N(\pm 1) = 1$ y $N(\pm 3) = 9$. Por otro lado $N((1-\omega)^4) = N^4(1-\omega) = 3^4 = 81$ y la norma es mayor que la de los dos anteriores.

Podemos suponer que es z quien es divisible por $1-\omega$, ya que la ecuación $x^3 + y^3 = z^3$ es equivalente a las ecuaciones $(-x)^3 + z^3 = y^3$ y $(-y)^3 + z^3 = x^3$. □

Ahora nos disponemos a terminar la demostración de nuestro teorema. Para ello volveremos a utilizar el método del descenso.

De entre todas las soluciones de $x^3 + y^3 = z^3$ donde $1-\omega$ divida a z, elijamos una solución de manera que la potencia de $1-\omega$ que divida a z sea mínima.

Recordemos que

$$(x+y)(\omega x + \omega^2 y)(\omega^2 x \omega y) = x^3 + y^3 = z^3.$$

Como $z^3 \equiv 0 \pmod{1-\omega}$ y $\mathbb{Z}[\omega]$ es un anillo de factorización única, uno de los factores $x+y, \omega x + \omega^2 y, \omega^2 x + \omega y$ es múltiplo de $1-\omega$.

Por otra parte,

$$x + y \equiv \omega x + \omega^2 y \equiv \omega^2 x + \omega y \equiv 0 \pmod{1-\omega}.$$

Entonces

$$\begin{cases} x + y & = (1-\omega)A \\ \omega x + \omega^2 y & = (1-\omega)B \\ \omega^2 x + \omega y & = (1-\omega)C \end{cases}.$$

De la relación $1 + \omega + \omega^2 = 0$ tenemos

$$(x+y) + (\omega x + \omega^2 y) + (\omega^2 x + \omega y) = (1-\omega)(A+B+C) = 0.$$

Seguidamente vamos a ver que $(A,B) = (A,C) = (B,C) = 1$. En efecto si $\gamma \mid (x+y)$ y $\gamma \mid (\omega x + \omega^2 y)$, entonces $\gamma \mid \omega(x+y)$ y $\gamma \mid (\omega x + \omega^2 y)$ y por tanto divide a la diferencia. Es decir $\gamma \mid y(1-\omega^2)$. También $\gamma \mid \omega^2(x+y)$. Restando de nuevo tenemos que $\gamma \mid x(1-\omega^2)$.

Como desde un principio hemos supuesto que $(x, y) = 1$, entonces γ tiene que ser necesariamente $1 - \omega$ o uno de sus asociados. Por lo tanto $(A, B) = 1$. De igual manera se demuestra el resto de los casos.

Podemos escribir la ecuación de la forma

$$z^3 = (x + y)(\omega x + \omega^2 y)(\omega^2 x + \omega y) = ABC(1 - \omega)^3.$$

Es decir,

$$\left(\frac{z}{1-\omega}\right)^3 = ABC \quad \text{con} \quad (A, B, C) = 1.$$

Como $\mathbb{Z}[\omega]$ es un anillo de factorización única tenemos que

$$A = \alpha\psi^3, \qquad B = \beta\xi^3, \qquad C = \gamma\theta^3,$$

donde α, β, γ son unidades y $\alpha\beta\gamma = \pm 1$.

Como $(x, y, z) = 1$, x e y no pueden ser múltiplos de $1-\omega$; y por el lema 5.1.5, si $x \equiv \pm 1 \pmod{1-\omega}$ entonces $x^2 \equiv \pm 1 \pmod{(1-\omega)^4}$. Igualmente para y.

Tenemos entonces que

$$x^3 + y^3 \equiv \pm 1 + \mp 1 \equiv 0 \pmod{(1-\omega)^4}.$$

(Recordemos que $x \equiv y \pmod{1-\omega}$).

Hemos demostrado así que A, B ó C deben ser múltiplos de $1-\omega$. Por ejemplo C.

$$C = \gamma\theta^3 = \gamma(1-\omega)^{3r}\theta_0^3.$$

Supongamos que $(1-\omega)^\lambda$ es la potencia de $1-\omega$ que divide a z. Entonces $3+3r = 3\lambda$ y por lo tanto $r = \lambda - 1$.

De la relación $A + B + C = 0$ tenemos

$$\alpha\psi^3 + \beta\xi^3 + \gamma\left((1-\omega)^{\lambda-1}\theta_0\right)^3 = 0.$$

Y casi hemos llegado a una solución donde el exponente donde el exponente de $1-\omega$ en z es menor que λ. Pero todavía nos estorban α, β y γ.

Como $A = \alpha\psi^3$ y $B = \beta\xi^3$ no son múltiplos de $1 - \omega$ entonces $\psi^3 \equiv \pm 1 \pmod{(1-\omega)^4}$ y $\xi^3 \equiv \pm 1 \pmod{(1-\omega)^4}$. De aquí,

$$\alpha\psi^3 + \beta\xi^3 + \gamma\theta^3 \equiv \pm\alpha \pm \beta \equiv 0 \pmod{(1-\omega)^3}.$$

Por otro lado sabemos que $\alpha\beta\gamma = \pm 1$. Como $\alpha = \pm\beta$, entonces $\pm\alpha^2\gamma = \pm 1$. Es decir, $\gamma = \pm\alpha = \pm\beta$.

Dividiendo la ecuación por β, las unidades que nos quedan son 1 ó -1, y ahora sí que las podemos meter dentro del paréntesís para obtener una solución que entra en contradicción con la hipótesis en el método del descenso. □

5.1.3. Representación de enteros como suma de dos cuadrados

En esta sección vamos a estudiar qué enteros son representables como suma de dos cuadrados.

En el capítulo 2 analizamos el comportamiento en media de la función

$$r(n)\#\{n = a^2 + b^2 : \ a, b \in \mathbb{Z}\}.$$

Concretamente vimos que

$$R(x) = \sum_{n \leq x} r(n) = \pi x + O(\sqrt{x}).$$

Sin embargo ahora vamos a considerar la ecuación $n = x^2 + y^2$ para un n dado y podremos saber el número de soluciones de dicha ecuación en función de la factorización de n en números primos.

Recordemos que el estudio de la factorización de $x^3 + y^3 = z^3$ lo hacíamos en $\mathbb{Z}[\omega]$ porque era allí donde $x^3 + y^3$ se podía factorizar.

No es de extrañar por tanto que el estudio de nuestra ecuación lo hagamos en $\mathbb{Z}[i]$, que es donde se puede factorizar $x^2 + y^2 = (x + iy)(x - iy)$.

Hagamos primeramente una serie de observaciones sobre el anillo $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$

1) $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$.

2) Las unidades de $\mathbb{Z}[i]$ son $\{\pm 1, \pm i\}$.

3) $\mathbb{Z}[i]$ es un anillo euclídeo y por tanto de factorización única.

4) Si $a + bi$ es primo en $\mathbb{Z}[i]$, entonces $a + bi$ divide a un primo racional.

5) Primos en $\mathbb{Z}[i]$. Después de 4), los primos en $\mathbb{Z}[i]$ los podemos buscar entre los divisores de los primos racionales.

   i) $p = 2$.
   Si $N(a + bi) = 2$, entonces $a + bi = 1 + i$ o cualquiera de sus asociados.

   ii) $p \equiv 3 \pmod 4$.
   Si p no fuese primo en $\mathbb{Z}[i]$, existirían a y b tales que $p = (a+bi)(a-bi) = a^2 + b^2$. Pero esto es imposible porque la suma de dos restos cuadráticos módulo 4 nunca puede ser 3.
   Todos los primos $p \equiv 3 \pmod 4$ en $\mathbb{Z}$, son también primos en $\mathbb{Z}[i]$.

a) $p \equiv 1 \pmod 4$.

En el capítulo de la Ley de Reciprocidad cuadrática vimos que si $p \equiv 1 \pmod 4$ entonces -1 era un residuo cuadrático módulo p. Entonces existirá un x tal que $x^2 \equiv -1 \pmod p$. Es decir $p \mid x^2+1 = (x+i)(x-i)$. Si p fuese primo en $\mathbb{Z}[i]$ debería dividir a alguno de estos factores. Pero ni $x/p + i/p$, ni $x(p - i/p$ son enteros en $\mathbb{Z}[i]$. Luego p tiene que tener algún divisor de la forma $a + bi$; $p = (a + bi)(a - bi) = a^2 + b^2$. Veremos ahora que $a + bi$ es primo en $\mathbb{Z}[i]$.

Si no fuese así tendríamos que $a + bi =)(c + di)(e + fi)$, donde la norma de los factores es mayor que 1. Pero eso es imposible $p = N(a + bi) = N(c + di)N(e + fi)$.

Resumiendo, hemos demostrado que los primos de $\mathbb{Z}[i]$ son $1 + i$, los primos racionales $p \equiv 3 \pmod 4$ y los divisores (que siempre existen) de los primos racionales $p \equiv 1 \pmod 4$.

Teorema 5.1.7. *Si*

$$n = 2^\alpha \prod_{p_j \equiv (4)} p_j^{r_j} \prod_{q_i \equiv 3(4)} q_i^{s_i},$$

entonces

$$r(n) = \begin{cases} 4\prod_j (1 + r_j) & \textit{si } s_i \textit{ es par para todo } i \\ 0 & \textit{en otro caso.} \end{cases}$$

Demostración. El primer paso será descomponer n en sus factores primos en $\mathbb{Z}[i]$:

$$^n = i^t (1 + i)^{2\alpha} \prod_j (a + bi)^{r_j} (a - bi)^{r_j} \prod_i q_i^{s_i}.$$

Buscamos el número de descomposiciones de n de la forma $n = A^2 + B^2 = (A + Bi)(A - Bi)$.

Cada uno de estos factores será de la forma

$$A + Bi = i^{t_1}(1 + i)^{\alpha_1} \prod_j (a + bi)^{r_{j,1}} (a - bi)^{r_{j,2}} \prod_i q_i^{s_{i,1}}$$

$$A - Bi = (-i)^{t_1}(1 - i)^{\alpha_1} \prod_j (a - bi)^{r_{j,1}} (a + bi)^{r_{j,2}} \prod_i q_i^{s_{i,1}}.$$

Igualando normas tenemos que

$$\begin{cases} \alpha_1 & = \alpha \\ r_{j,1} + r_{j,2} & = r_j \\ 2s_{i,1} & = s_i. \end{cases}$$

De aquí se sigue que una condición necesaria para que n sea suma de dos cuadrados es que todos los s_i sean pares.

En ese caso tendremos, para cada j, $r_j + 1$ posibles elecciones de los $r_{j,1}$ y cuatro posibles elecciones de t_1, lo que demuestra el teorema. □

5.1.4. Suma de cuatro cuadrados

Hemos visto que hay números que no se pueden escribir como suma de dos cuadrados y es un ejercicio comprobar que si $n \equiv 7 \pmod 8$ entonces n no se puede escribir como suma de tres cuadrados. ¿Será la suma de cuatro cuadrados suficiente para representar cualquier entero?

Teorema 5.1.8 (Lagrange)**.** *Todo número natural puede expresarse como suma de cuatro cuadrados.*

Demostración. Después del siguiente lema, bastará con demostrar que todo primo p es suma de cuatro cuadrados.

Lema 5.1.9 (Euler)**.** *Si $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ y $m = y_1^2 + y_2^2 + y_3^2 + y_4^2$, entonces*

$$nm = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

para algunos enteros z_1, z_2, z_3, z_4.

Demostración. Basta con comprobar la relación

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2\\ &+(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

□

Lema 5.1.10. *Sea p primo impar. Entonces existe un m, $1 \leq m < p$ tal que*

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Demostración. Consideremos los conjuntos

$$S_1 = \{0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$$

$$S_2 = \{-0^2, -1^2, \ldots, -\left(\frac{p-1}{2}\right)^2 - 1\}.$$

Los elementos de S_1 son incingruentes entre sí módulo p. En efecto, si $x^2 \equiv y^2 \pmod{p}$ entonces $p \mid (x-y)(x+y)$. Pero eso es imposible porque $0 < x-y < x+y < p$.

Por la misma razón los elementos de S_2 también son incongruentes entre sí. Ambos conjuntos tienen $\frac{p+1}{2}$ elementos. Como entre los dos tienen $p+1$ elementos, dos de ellos, uno de S_1 y otro e S_2, han de ser incongruentes entre sí.

$$x^2 \equiv -y^2 - 1 \pmod{p}.$$

Es decir, $x^2 + y^2 + 1^2 + 0^2 = mp$. Sólo falta por ver que $m < p$. Pero esto sigue de la relación

$$m = \frac{x^2+y^2+1}{p} \leq \frac{(\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1}{p} < p.$$

□

La conclusión del teorema de Lagrange es consecuencia del siguiente lema.

Lema 5.1.11. *Si m es el menor entero que verifica el lema anterior entonces $m = 1$.*

Demostración. Sea m el mínimo entero tal que $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Si m es par tenemos las siguientes posibilidades: todos los x_i son impares, todos los x_i son pares o exactamente dos x_i son pares y los otros dos impares.

En cualquier caso podríamos escribir

$$\frac{m}{2}p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2.$$

Todos los números en el interior de los paréntesis son enteros, así como $\frac{m}{2}$. Pero entonces $\frac{m}{2}$ verificaría el lema anterior y ya no sería m el mnor número que lo hiciera.

Por lo tanto hemos demostrado que m ha de ser impar. Nuestro objetivo es demostrar que $m = 1$. Vamos a suponer que $m \geq 3$ y llegaremos a una contradicción.

Definamos los y_i de la manera siguiente:

$$y_i \equiv x_i \pmod{m}, \qquad -\frac{m-1}{2} \leq y_i \leq \frac{m-1}{2}.$$

De manera obvia se verifica

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}.$$

Escribamos

$$mn = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4\left(\frac{m-1}{2}\right)^2 < m^2.$$

Es decir, $n < m$.

Si $n = 0$, $y_1 = y_2 = y_3 = y_4 = 0$ y entonces $x_i \equiv 0 \pmod{m}$ y por lo tanto $x_i^2 \equiv 0 \pmod{m^2}$. Luego

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 = km^2$$

y $p = km$ con $1 < m < p$, lo cual es imposible porque p es primo.

Entonces podemos suponer que $n > 0$. Hagamos el siguiente producto utilizando el lema 5.1.9:

$$m^2pn = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2.$$

Como $x_i \equiv y_i \pmod{m}$, tenemos

$$\begin{aligned}
z_2 &\equiv x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\
&\equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod{m} \\
z_3 &\equiv x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\
&\equiv x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4 \equiv 0 \pmod{m} \\
z_4 &\equiv x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \\
&\equiv x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2 \equiv 0 \pmod{m} \\
z_1 &\equiv x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\
&\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}
\end{aligned}$$

Ahora podemos escribir

$$pn = \left(\frac{z_1}{m}\right)^2 + \left(\frac{z_2}{m}\right)^2 + \left(\frac{z_3}{m}\right)^2 + \left(\frac{z_4}{m}\right)^2$$

donde los z_i/m son enteros.

Es decir, hemos encontrado un $n < m$ que verifica la hipótesis inicial y contradice el hecho de que m sea el menor entero que la cumple. Por lo tanto hemos completado la demostración. □

□

El teorema de Lagrange es un caso particular del problema de Waring, que consiste en hallar, para cada $k \geq 2$, el menor entero $g(k)$ con la propiedad de que todo entero positivo se puede escribir como suma de $g(k)$ k-potencias. Hilbert demostró que $g(k)$ existe para todo $k \geq 2$ y el teorema de Lagrange demuestra que $g(2) = 4$. Como una aplicación del teorema de Lagrange demostraremos que $g(4) \leq 53$.

Teorema 5.1.12. *Todo entero positivo puede expresarse como suma de* 53 *cuartas potencias.*

Demostración.

Lema 5.1.13.

$$6\left(\sum_{i=1}^{4} x_i^2\right)^2 = \sum_{1\leq i<j\leq 4} (x_i + x_j)^4 + (x_i - x_j)^4.$$

Demostración. Es una simple comprobación. □

EL teorema de Lagrange nos dice que todo número natural se puede escribir como suma de cuatro cuadrados. Luego todo múltiplo de 6 se podrá escribir de la forma $6n_1^2 + 6n_2^2 + 6n_3^3 + 6n_4^2$. Ya cada uno de los sumandos, por el lema anterior, se puede escribir como suma de 12 cuartas potencias. Es decir, todo múltiplo de 6 puede escribirse como suma de 48 cuartas potencias.

Para finalizar, si $n = 6k + r,\ 0 \leq r < 6$, entonces

$$n = 6k + r = \sum_{i=1}^{48} z_i^4 + \sum_{j=1}^{r} 1^4.$$

En el pero de los casos necesitaremos 53 cuartas potencias. □

5.2. Ejercicios del capítulo 6

5.2.1. *Hallar todas las ternas de cuadrados en progresión aritmética.*

5.2.2. *Demostrar que la ecuación* $x^2 + y^2 = 7z^2$ *no tiene soluciones en enteros positivos.*

5.2.3. *Demostrar que si un triángulo rectángulo tiene lados de longitud entera entonces la suma de los lados divide al producto de los mismos.*

5.2.4. *Hallar todas las soluciones enteras de la ecuación* $x^2 + y^2 = z^4$.

5.2.5. *Hallar todas las soluciones en enteros positivos de la ecuación* $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$.

5.2.6. *Hallar todas las soluciones en enteros positivos de la ecuación* $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$.

5.2.7. *Demostrar que la ecuación* $\frac{1}{x^4} + \frac{1}{y^4} = \frac{1}{z^2}$ *no tiene soluciones enteras.*

5.2.8. *Probar que* $x^4 + 4y^4 = z^2$ *no tiene soluciones con* $xy \neq 0$.

5.2.9. *Probar que* $x^4 - y^4 = z^2$ *no tiene soluciones con* $yz \neq 0$.

5.2.10. *Hallar todas las soluciones en enteros positivos de la ecuación* $11050 = x^2 + y^2$.

5.2.11. *Demostrar que la única solución en enteros positivos de la ecuación* $y^2 = x^3 - 1$ *es* $y = 3,\ x = 2$.

Capítulo 6

Aproximación de números reales por racionales

En la antigua Grecia los números tenían un carácter mágico y divino. EL primer lugar de la jerarquía lo ocupaban los números primos, después el resto de los números enteros. Había otros sin el mismo grado de perfección, los que se expresan como cociente de dos enteros. Entonces parecía inconcebible que existiera otra clases de números. Cuenta la leyenda que el primer matemático que demosttró que la diagonal de un cuadrado de lado 1 no puede ser el cociente de dos enteros, pagó muy cara su herejía.

Estamos en otros tiempos y podemos empezar este capítulo demostrando que $\sqrt{2}$ es un número irracional.

Teorema 6.0.12. *$\sqrt{2}$ es irracional.*

Demostración. Si $\sqrt{2} = a/b$ entonces $2b^2 = a^2$. Pero entonces el exponente de 2 de la parte izquierda es impar, mientras el del de la derecha es par. □

Después de este sencillo ejercicio a estudiar cómo se aproximan los números reales por racionales.

6.1. Aproximación de números reales por racionales

Proposición 6.1.1. *Sea θ real y $N > 1$. Entonces existe un racional $\frac{h}{k}$, $k \leq N$ tal que $\left|\theta - \frac{h}{k}\right| < \frac{1}{kN}$.*

Demostración. Si $\theta = \frac{p}{q}$, con $q \leq N$ entonces $\left|\theta - \frac{p}{q}\right| = 0 \leq \frac{1}{kN}$.

Si $\theta = \frac{p}{q}$ con $q > N$ ó θ es irracional, construyamos los números $(m\theta) = m\theta - [m\theta],\ m = 1, \ldots, N$.

Ahora aplicamos el principio del palomar al intervalo $[0, 1]$ dividido en N trozos de longitud $1/N$.

$$[0, 1/N),\ [1/N, 2/N), \ldots, [(N-1)/N, 1).$$

Si existe un m tal que $(m\theta)$ está en el primer intervalo, tendríamos $|m\theta - [m\theta]| < 1/N$, Dividiendo entre m obtenemos la aproximación deseada:

$$\left|\theta - \frac{[m\theta]}{m}\right| < \frac{1}{mN}.$$

SI no existiera tal m, tendríamos N números en $N-1$ intervalos. Luego dos de ellos, $(m\theta)$ y $(m'\theta)$ tendrían que estar en el mismo intervalo, por lo que su distancia sería menor que $1/N$,

$$|m\theta - [m\theta] - (m'\theta - [m'\theta])| < \frac{1}{N}.$$

Dividiendo entre $m - m'$ obtenemos el resultado deseado:

$$\left|\theta - \frac{[m\theta] - [m'\theta]}{m - m'}\right| < \frac{1}{(m - m')N}.$$

□

Proposición 6.1.2. *El número θ es irracional si y sólo si existen infinitas fracciones $\frac{a}{b}$ tales que $\left|\theta - \frac{a}{b}\right| < \frac{1}{b^2}$.*

Demostración. Por la proposición anterior sabemos que para cada n existe una fracción $\frac{a_n}{b_n}$ tal que

$$\left|\theta - \frac{a_n}{b_n}\right| < \frac{1}{nb_n}$$

con $b_n \leq n$. Entonces $\left|\theta - \frac{a_n}{b_n}\right| < \frac{1}{b_n^2}$.

Si sólo hubiese un número finito de fracciones $\frac{a_n}{b_n}$ cumpliendo dicha propiedad, una misma fracción tendrían lugar para infinitos n: $\frac{a_n}{b_n} = \frac{a}{b}$ para infinitos n. Es decir,

$$\left|\theta - \frac{a}{b}\right| < \frac{1}{bn}$$

para infinitos valores de n, y tendríamos que $\theta = \frac{a}{b}$.

En el otro sentido, supongamos que $\theta = \dfrac{p}{q}$, $(p,q) = 1$, es un racional y que existen infinitos racionales $\dfrac{a}{b}$ tales que si $\left|\dfrac{p}{q} - \dfrac{a}{b}\right| < \dfrac{1}{b^2}$. Como $\dfrac{1}{bq} \leq \left|\dfrac{p}{q} - \dfrac{a}{b}\right|$ para $\dfrac{a}{b} \neq \dfrac{p}{q}$ entonces necesariamente tenemos que $b < q$, lo que limita a un número finito las posibilidades de los racionales $\dfrac{a}{b}$. □

El resultado de la proposición 6.1.2 puede ser mejorado en el sentido de sustituir $|\theta - \frac{a}{b}| < \frac{1}{b^2}$ por $|\theta - \frac{a}{b}| < \frac{1}{\sqrt{5}b^2}$, que es la mejor constante posible.

Demostrar que un número real es irracional puede constitutir un problema muy difícil. La siguiente observación nos puede ayudar en algunos casos.

Si $\frac{P}{Q}$, $\frac{p}{q}$ son racionales distintos es claro que

$$\left|\frac{P}{Q} - \frac{p}{q}\right| = \frac{|Pq - pQ|}{Qq} \geq \frac{1}{Qq}.$$

Por lo tanto para ver que un número θ es irracional basta con obtener una sucesión de racionales $\frac{p_n}{q_n}$ tales que

$$\left|\theta - \frac{p_n}{q_n}\right| = o\left(\frac{1}{q_n}\right).$$

6.2. Irracionalidad de π y de e^m

La estrategia sugerida anteriormente para ver si un número es irracional no siempre es fácil de aplicar. Afortunadamente las propiedades intrínsecas de ciertos números nos permiten combinarla con otro tipo de argumentos 'para demostrar que son irracionales.

Teorema 6.2.1. *π es irracional.*

Demostración. Supongamos que π es racional, $\pi = \dfrac{n}{m}$. Consideremos el polinomio $p(x) = x(n - mx)$.

Veamos primero que $D_x^j\left(\dfrac{p^k(x)}{k!}\right)$ es un entero en $x = 0$ y en $x = \pi$.

$$D_x^j\left(\frac{p^k(x)}{k!}\right) = D_x^j\left(\frac{1}{k!}x^k(n - mx)^k\right) = \frac{1}{k!}\sum_{0\leq r\leq k}\sum_{0\leq s\leq k} a_{r,s}x^r(n - mx)^s$$

para ciertos enteros $a_{r,s}$.

Si $r > 0$ y $s > 0$, entonces $\frac{1}{k!}a_{r,s}x^r(n-mx)^s$ se anula en $x = 0$ y en $x = \pi = n/m$.

Si $r = 0$, entonces x^k ha sido derivado por lo menos k veces y por lo tanto $k!$ debe dividir a $a_{0,s}$.

Tenemos entonces que $\frac{1}{k!}a_{0,s}(n-mx)^s$ es entero en $x = 0$ y en $x = n/m$.

Por último, si $s = 0$, $a_{r,0}$ será múltiplo de $m^k k!$ por la misma razón anterior. En este caso $\frac{1}{k!}a_{r,0}x^r$ también es entero en $x = 0$ y en $x = n/m$ porque $r \leq k$.

Una vez visto esto pasemos a demostrar nuestro teorema. Por definición

$$e^{p(x)} = \sum_{k=0}^{\infty} \frac{p^k(x)}{k!}.$$

Entonces

$$\int_0^\pi \sin x \; e^{p(x)} dx = \sum_{k=0}^{\infty} \int_0^\pi \sin x \; \frac{p^k(x)}{k!} dx.$$

Integrando por partes tenemos

$$\int_0^\pi \sin x \; \frac{p^k(x)}{k!} dx = -\cos x \left(\frac{p^k(x)}{k!}\right)' \Big|_0^\pi + \int_0^\pi \cos x \left(\frac{p^k(x)}{k!}\right)' dx.$$

Integrando otra vez por partes,

$$\int_0^\pi \cos x \left(\frac{p^k(x)}{k!}\right)' dx = \sin x \left(\frac{p^k(x)}{k!}\right)'' \Big|_0^\pi - \int_0^\pi \sin x \left(\frac{p^k(x)}{k!}\right)'' dx.$$

En un número finito de pasos obtendremos $\int_0^\pi \sin x \; \frac{p^k(x)}{k!}$ como una suma finita de términos de la forma $\sin x \left(\frac{p^k(x)}{k!}\right)^{j)} \Big|_0^\pi$ y $\cos x \left(\frac{p^k(x)}{k!}\right)^{j)} \Big|_0^\pi$.

Como las funciones $\sin x$, $\cos x$ y $\left(\frac{p^k(x)}{k!}\right)^{j)}$ toman valores enteros en $x = 0$ y $x = \pi$, el valor de la integral será un número entero para todo k.

Además las funciones $\sin x$ y $\frac{p^k(x)}{k!}$ son estrictamente positivas en el intervalo $(0, \pi)$. Luego la integral $\int_0^\pi \sin x \; \frac{p^k(x)}{k!} dx$ debe ser un número entero mayor o igual que 1.

Por tanto la integral $\int_0^\pi \sin x \; e^{p(x)}$ debería ser infinita, lo cual es absurdo porque estamos integrando sobre un intervalo finito una función acotada en dicho intervalo. □

Teorema 6.2.2. *El número e^m es irracional para todo entero $m \neq 0$.*

Demostración. Consideremos el polinomio $p(x) = x(m-x)$. Por las mismas razones que en el teorema anterior, $D_x^j\left(\frac{p^k(x)}{k!}\right)$ toma valores enteros en $x = 0$ y en $x = m$.

También tenemos

$$\int_0^m e^x e^{p(x)} dx = \int_0^m e^x \sum_{k=0}^{\infty} \frac{p^k(x)}{k!} dx = \sum_{k=0}^{\infty} \int_0^m e^x \frac{p^k(x)}{k!} dx.$$

Integrando por partes,

$$\int_0^m e^x \frac{p^k(x)}{k!} dx = e^x \left(\frac{p^k(x)}{k!}\right)' \Big|_0^m - \int_0^m e^x \left(\frac{p^k(x)}{k!}\right)' dx.$$

Repitiendo el proceso un número finito de veces, el valor de la integral para cada k será de la forma $e^m z_1 + z_2,\ z_1, z_2 \in \mathbb{Z}$.

También cada una de las integrales es estrictamente positiva porque las funciones e^x y $p^k(x)$ son estrictamente positivas en el intervalo $(0, m)$.

Si e^m fuese racional, $e^m = \frac{a}{b}$, entonces $e^m z_1 + z_2 \geq \dfrac{1}{b}$ y

$$\int_0^m e^x e^{p(x)} dx \geq \sum_0^{\infty} \frac{1}{b} = \infty$$

lo cual es absurdo porque la integral es finita. □

Curiosamente, aunque casi todos los números son irracionales, son pocos los que se conocen explícitamente. En general es un problema muy difícil demostrar la racionalidad o irracionalidad de un número real dado.

Por ejemplo se desconoce si la constante de Euler,

$$\gamma = \lim_{k\infty} \left(\sum_{n=1}^{k} - \log k\right)$$

es un número irracional, y en la misma situación se encuentra el número π^e.

6.3. Números algebraicos y trascendentes

Dentro de los números irracionales, hay algunos más irracionales que otros.

Un número irracional es aquél que no satisface ninguna ecuación polinómica de grado 1 con coeficientes enteros. Por ejemplo, $\sqrt{2}$. Sin embargo este número satisface

una ecuación polinómica de grado 2, $x^2 - 2 = 0$ y, de alguna manera, podemos decir que es menos irracional que por ejemplo $\sqrt[3]{2}$, que satisface una ecuación polinómica de grado 3.

Definicion 6.3.1. *Un número α es un número algebraico de orden n si es raíz de un polinomio irreducible de grado n con coeficientes enteros.*

¿Existen números reales que no son algebraicos de ningún orden? La respuesta es afirmativa. De hecho sabemos mucho más: el conjunto de los números algebraicos es numerable y, por tanto, en el sentido de la teoría de la medida de Lebesgue casi ningún punto es algebraico. Si escogemos al azar un punto de la recta real, con probabilidad igual a 1 se corresponderá con un número no algebraico.

A estos números no algebraicos les llamaremos trascendentes.

Teorema 6.3.2 (Liouville)**.** *Si α es un número algebraico de orden $n \geq 2$, existe una constante $C_\alpha > 0$ tal que*

$$\left|\alpha - \frac{p}{q}\right| > \frac{C_\alpha}{q^n}$$

para todo par de enteros p, q.

Demostración. Si α es algebraico de orden n, existirá un polinomio irreducible $f(x)a_n x^n + \cdots + a_1 x + a_0$ tal que $f(\alpha) = 0$.

Sea $M = \sup_{\alpha-1<x<\alpha+1} |f'(x)|$. Si $\left|\alpha - \frac{p}{q}\right| < 1$, por el teorema del valor medio tenemos que para algún $x \in (\alpha - 1, \alpha + 1)$,

$$\left|f(\alpha) - f(\frac{p}{q})\right| = \left|\alpha - \frac{p}{q}\right| |f'(x)| \leq \left|\alpha - \frac{p}{q}\right| M.$$

Como $f(\alpha) = 0$, tenemos

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{|f(p/q)|}{M}.$$

Sustituyendo en el polinomio, $f(p/q)$ es un número racional con denominador menor o igual que q^n y distinto de 0 por ser irreducible. Entonces

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1/M}{q^n}$$

y el teorema está demostrado tomando $C_\alpha = 1/M$. □

El estudio de la trascendencia de un número es bastante más difícil que el estudio de su irracionalidad.

Sabemos que π y e son números trascendentes. La trascendencia de π fue demostrada por Lindemann, acabando así con el famosi porblema de la cuadratura del círculo: a partir de un círculo de diámetro 1, ¿podemos construir con regal y compás un cuadrado del mismo área? Esto equivaldría a construir el número $\sqrt{\pi}$. Ahora bien las construcciones con regla y compás involucran la resolución de ecuaciones de primer grado, intersección de dos rectas, o de segundo grado, intersección de una recta y una circunferencia o de dos circunferencias entre sí. Si un número es construible entonces es raíz de un polinomio irreducible (en $\mathbb{Z}$) con coeficientes enteros de grado igual a una potencia de 2.

Como $\sqrt{\pi}$ es trascendente, en particular no puede ser construible y por lo tanto no podemos cuadrar el círculo.

Teorema 6.3.3 (Hermite)**.** *El número e es trascendente.*

Demostración. Supongamos, por el contrario, que es algebraico y que satisface la ecuación

$$a_n e^n + a_{n-1} e^{n-1} + \cdots + a_1 e + a_0 = 0$$

de coeficientes enteros, con $a_0 \neq 0$ y $a_n \neq 0$.

Fijado un número primo p construimos el polinomio

$$P(x) = x^{p-1}(x-1)^p \cdots (x-n)^p$$

y la función

$$I(y) = \int_0^y e^{y-x} P(x) dx, \qquad y \geq 0.$$

Integrando por partes repetidas veces obtenemos la expresión

$$I(y) = e^y \sum_{j=0}^{d} P^{j)}(0) - \sum_{j=0}^{d} P^{j)}(y)$$

donde $d = (n+1)p - 1$ es el grado del polinomio $P(x)$.

Consideremos la cantidad

$$A = a_0 I(0) + \cdots + a_n I(n) = \sum_{j=0}^{d} \sum_{k=0}^{n} a_k \left(e^k P^{j)}(0) - P^{j)}(k) \right) = -\sum_{j=0}^{d} \sum_{k=0}^{n} a_k P^{j)}(k).$$

Tenemos que:

1) $P^{j)}(k)$ es un múltiplo de $p!$ si $j \geq p$.

2) $P^{j)}(k) = 0$ si $j < p$ y $1 \leq k \leq n$ ó si $j < p-1$ y $k = 0$.

3) $P^{j)}(k)$ es un entero divisible por $p!$ excepto en el caso $j = p-1,\ k = 0$.

4) $P^{p-1)}(0) = (p-1)!(-1)^{np}(n!)^p$. Luego , si $p > n$ entonces $P^{p-1)}(0)$ es un entero divisible por $(p-1)!$ pero no por $p!$.

Recapitulemos: si $p > n$ entonces A es un entero distinto de cero y divisible por $(p-1)!$.

Por otro lado, de la definición de la función $I(y)$ se obtiene fácilmente la estimación:

$$|I(y)| \leq ye^y \sup_{0 \leq x \leq y} |P(x)| \leq ye^y(n+y)^d.$$

Luego

$$\begin{aligned} |A| \leq \sum_{j=1}^{n} |a_j||I(j)| &\leq \max_j |a_j| \sum_{j=1}^{n} je^j(n+j)^d \leq \max_j |a_j| e^n n^2 (2n)^d \\ &\leq \max_j |a_j| e^n n^2 (2n)^{(n+1)p-1} \leq C^p \end{aligned}$$

para alguna constante positiva $C = C(n)$.

Si p es suficientemente grande resulta absurdo que $(p-1)! \ll C^p$. □

6.4. Sucesiones uniformemente distribuidas

Definicion 6.4.1. *Decimos que una sucesión de números reales* $\{a_n\} \subset [0,1]$ *está uniformemmente distribuida si para todo intervalo* $I \subset [0,1]$,

$$\lim_{N \to \infty} \frac{\#\{a_j \in I,\ j = 1, 2 \ldots, N\}}{N} = |I|.$$

Esto es lo mismo que decir que

$$\lim_{N \to \infty} \frac{1}{N} \sum_{j=1}^{N} \chi_I(a_j) = |I|,$$

donde χ_I es la función característica del intervalo I.

Teorema 6.4.2 (H. Weyl)**.** *Si* θ *es un número irracional entonces la sucesión* $\{(n\theta)\}$ *está uniformemente distribuida en* $[0,1]$.

Vamos a descomponer en varias etapas la demostración de este teorema.

Una partición del intervalo $[0,1]$ es un conjunto de puntos $0 = t_0 < t_1 < \cdots < t_n = 1$.

Una función acotada y definida en $[0,1]$, es continua y definida a trozos si existe una partición $0 = t_0 < t_1 < \cdots < t_n = 1$ del intervalo $[0,1]$ de manera que la restricción de f a cada intervalo $[t_{i-1}, t_i),\ i = 1, \ldots, n$ sea una función continua.

El caso en el que la función continua a trozos es igual a una constante en cada intervalo $[t_{i-1}, t_i)$ recibe un nombre especial, se dice que f es una función escalonada. Es decir, f es escalonada si es de la forma

$$f(x) = \sum_{k=1}^{n} a_k \chi_{[t_{k-1}, t_k)}(x) \qquad \text{donde}$$

$$\chi_{[t_{k-1}, t_k)}(x) = \begin{cases} 1 \text{ si } x \in [t_{k-1}, t_k) \\ 0 \text{ en otro caso.} \end{cases}$$

Lema 6.4.3. *Una condición necesaria y suficiente para que una sucesión* $\{a_n\} \subset [0,1]$ *esté uniformemente distribuida en* $[0,1]$ *es que*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(a_k) = \int_0^1 f(x)dx$$

para toda función f *continua a trozos.*

Demostración. i) Si la igualdad (6.4.3) es cierta para toda función continua a trozos, en particular es cierta para la función característica de un intervalo $I = [a,b) \subset [0,1)$, es decri:

$$\lim_{n\to\infty} \frac{\#\{a_j \in I, \quad j = 1, 2, \ldots, n\}}{n} = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \chi_{[a,b)}(a_k) = \int_0^1 \chi_{[a,b)}(x)dx = b - a$$

ii) El hecho de que $\{a_n\}$ esté distribuida uniformemente es equivalente a afirmar que la igualdad (6.4.3) es cierta para funciones escalonadas. Basta con observar que toda función continua a trozos puede aproximarse por funciones escalonadas; es decir, que para todo $\epsilon > 0$ podemos encontrar funciones escalonadas f_1 y f_2 tales que $f_1 \leq f \leq f_2$ y $\int_0^1 (f_2(x) - f_1(x))dx \leq \epsilon$. Por tanto

$$\limsup_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(a_k) \leq \lim_{n\to\infty} f_2(a_k) = \int_0^1 f_2(x) \leq \int_0^1 f(x)dx + \epsilon.$$

$$\liminf_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} f(a_k) \geq \lim_{n\to\infty} f_1(a_k) = \int_0^1 f_1(x) \geq \int_0^1 f(x)dx - \epsilon.$$

□

Teorema 6.4.4. *Una condición suficiente y necesaria para que la sucesión* $\{a_n\}$ *esté uniformemente distribuida en el intervalos* $[0,1]$ *es que*

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} e^{2\pi i m a_k} = 0$$

para todo entero $m \neq 0$.

Demostración. a) La condición es necesaria: Para probarlo, como $e^{ix} = \cos x + i \sin x$, basta con aplicar el lema 6.4.3 a las funciones $f(x) = \cos(2\pi mx)$ y $f(x) = \sin(2\pi mx)$ y observar que

$$\int_0^1 \cos(2\pi mx)dx = \int_0^1 \sin(2\pi mx)dx = 0$$

si $m \in \mathbb{Z},\ m \neq 0$.

b) La suficiencia es un poco más delicada y está basada en el hecho de que toda función continua f en el intervalo $[0,1]$ tal que $f(0) = f(1)$ puede aproximarse uniformemente por polinomios trigonométricos de la forma

$$P(x) = b_0 + (b_1 \cos(2\pi x) + c_1 \sin(2\pi x) + \cdots + (b_m \cos(2\pi mx) + c_m \sin(2\pi mx)$$

Si

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{m} \cos(2\pi m a_k) + i \sin(2\pi m a_k) = 0$$

para todo $m > 0$, entonces

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} P(a_k) = b_0 = \int_0^1 P(x)dx$$

para todo polinomio trigonométrico $P(x)$ y, por lo expuesto anteriormente,

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} f(a_k) = \int_0^1 f(x)dx$$

para toda función continua.

Finalmente basta con observar que si f es continua a trozos, podemos encontrar dos funciones continuas y periódicas tales que $f_1 \leq f \leq f_2$ y $\int_0^1 (f_2(x) - f_1(x))dx \leq \epsilon$. □

Demostración del teorema 6.4.2. Tenemos que probar que para todo entero positivo m,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} e^{2\pi i m(n\theta)} = 0.$$

Utilizaremos el hecho de que $e^{2\pi i m(n\theta)} = e^{2\pi i m n\theta}$ y que $\sum_{k=1}^{n} e^{2\pi i k x} = \frac{e^{2\pi i x} - e^{2\pi i (n+1)x}}{1-e^{2\pi i x}}$ cuando x no es un entero.

Al ser θ irracional $m\theta$ nunca va a ser un entero y entonces

$$\left| \frac{1}{n} \sum_{k=1}^{n} e^{2\pi i m(n\theta)} \right| = \frac{1}{n} \left| \frac{e^{2\pi i m\theta} - e^{2\pi i (n+1) m\theta}}{1 - e^{2\pi i m\theta}} \right| \leq \frac{1}{n} \frac{2}{|1 - e^{2\pi i m\theta}|},$$

que tiende a cero cuando $n \to \infty$. □

Hacer estimaciones no triviales del tipo $\sum e^{2\pi i a_j}$ es un instrumento clave para resolver muchos problemas en teoría de números.

Po ejemplo, la sucesión $(n^k\theta)$ se trata en el problema de Waring, y la sucesión $(p\theta)$ donde p recorre los primos, en la conjetura de Goldbach.

El teorema de H. Weyl, y sus extensiones a dimensiones mayores, es un resultado importante no sólo en la teoría de los Números, sino también en Geometría y Sistemas dinñamicos.

En el párrafo siguiente consideraremos otra generalización del caso $(a_n x)$, $a_n \to \infty$ que es válida para casi todos los números $x \in (0, 1]$, en el sentido de la teoría de la medida.

6.4.1. Números normales

Dado el número real $x \in [0, 1)$ con desarrollo decimal $x = 0, x_1 x_2 \ldots x_k \ldots$, y dado un dígito $m \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, el número

$$\frac{\#\{x_j = m,\ j = 1, \ldots, N\}}{N}$$

mide la frecuencia con la que el dígito m aparece en al sucesión de las N primeras cifras decimales de x.

Definicion 6.4.5. *Un número $x \in [0, 1)$ será llamado normal si, para todo dígito m, existe*

$$\lim_{N\to\infty} \frac{\#\{x_j = m,\ j = 1, \ldots, N\}}{N} = \frac{1}{10}.$$

En otras palabras, un número normal es aquel que tiene la misma proporción de cada uno de los dígitos en su desarrollo decimal.

Es fácil construir números normales, como $0,1234567890123456789012..$ y no normales, por ejemplo, $0,121212\ldots$ El siguiente teorema de E. Borel tiene conexiones interesantes con otras ramas de las Matemáticas, tales como la Teoría Ergódica y la Probabilidad.

Teorema 6.4.6. *Excepto por un conjunto de medida cero, todos los números son normales.*

La demostración la vamos a basar en una extensión del Teorema de H. Weyl.

Teorema 6.4.7. *Sea $\{a_n\}$ una sucesión creciente de números enteros. Para casi todo número real x (es decir, excepto por un conjunto de medida igual a cero), la sucesión $(a_n x)$ está uniformemente distribuida en el intervalo $[0,1)$.*

Demostración. Fijado el número entero $m \neq 0$, consideremos las sumas

$$S_M(x) = \frac{1}{M}\sum_{n=1}^{M} e^{2\pi i m a_n x}$$

y la integrales

$$\int_0^1 |S_M(x;m)|^2 dx = \frac{1}{M^2}\sum_{n,k=1}^{M}\int_0^1 e^{2\pi i m(a_n-a_k)x}dx = \frac{1}{M},$$

ya que si $n \neq k$, entonces $\int_0^1 e^{2\pi i m(a_n-a_k)x}dx = 0$.

Por lo tanto, si consideramos la serie

$$F(x;m) = \sum_{N=1}^{\infty} |S_{N^2}(x;m)|^2$$

resulta que

$$\int_0^1 F(x;m)dx = \lim_{k\to\infty}\int_0^1 \sum_{N=1}^{k} |S_{N^2}(x;m)|^2 dx = \sum_{N=1}^{\infty}\frac{1}{N^2} < \infty.$$

Por lo tanto, para cada entero $m \neq 0$, ha de verificarse que $F(x;m) < \infty$ en casi todo x; es decir, excepto en un conjunto B_m de medida cero.

En particular, si $x \notin B_m$ entonces $\lim_{N\to\infty} S_{N^2}(x;m) = 0$.

Dado el entero positivo M podemos encontrar $N = [\sqrt{M}]$ tal que $N^2 \leq M < (N+1)^2$. Entonces

$$S_M(x;m) = \frac{1}{M}\left\{\sum_{n=1}^{N^2} e^{2\pi i m a_n x} + \sum_{n=N^2+1}^{M} e^{2\pi i m a_n x}\right\}$$

y

$$|S_M(x;m)| \leq |S_{N^2}(x;m)| + \frac{2N+1}{M}.$$

Luego si $x \notin B_m$ tenemos que

$$\lim_{M\to\infty} S_M(x;m) = 0.$$

Finalmente el conjunto $B = \bigcup_{m\neq 0} B_m$ es de medida cero y verifica que si $x \notin B$ entonces

$$\lim_{M\to\infty} \frac{1}{M}\sum_{n=1}^{M} e^{2\pi i m a_n x} = 0$$

para todo $m \neq 0$. En particular la sucesión $(a_n x)$ está uniformemente distribuida en $[0,1)$. □

Demostración del teorema 6.4.6. Consideremos la sucesión $a_n = 10^n$. Según el teorema anterior, existe un conjunto de medida cero B tal que si $x \notin B$ entonces $(10^n x)$ está uniformemente distribuida.

Dado el dígito $k = 0, 1, \ldots, 9$ consideremos el intervalo $I_k = [\frac{k}{10}, \frac{k+1}{10})$. La condición de distribución uniforme implica que

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} \chi_{I_k}(10^n x) = \int_0^1 \chi_{I_k}(x)dx = \frac{1}{10}.$$

La demostración se concluye observando que si $0, x_1 x_2 \ldots x_n \ldots$ es el desarrollo decimal del número x, entonces $(10^n x) = 0, x_{n+1} \ldots$ Es decir, $(10^n x) \in I_k$ si y sólo si $x_{n+1} = k$. □

6.5. Ejercicios

6.5.1. *Demostrar que $\sqrt[3]{3} - \sqrt{2}$ es irracional.*

6.5.2. *Demostrar que el logaritmo decimal de un racional positivo, o bien es entero, o bien es irracional.*

6.5.3. *Demostrar que si existen infinitas fracciones* $\frac{a_n}{b_n}$ *tales que* $\lim_{n\to\infty} b_n \left|\theta - \frac{a_n}{b_n}\right| = 0$*, entonces* α *es irracional. Como aplicación demostrar que* e *es irracional.*

6.5.4. *Sea* $p(n)$ *un polinomio con coeficientes enteros y positivos. Demostrar que* $\sum_{n=1}^{\infty} \frac{1}{10^{p(n)}}$ *es racional si y sólo si* $p(n)$ *es de grado* 1*.*

6.5.5. *Demostrar que* $\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{4q^2}$ *para todo par de enteros* p, q*.*

6.5.6. *Hallar tres fracciones* a/b *tales que* $|\sqrt{6} - a/b| < b^{-2}$*.*

6.5.7. *Demostrar que* $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ *es trascendente.*

6.5.8. *Sea* $\alpha = \sum_n 5^{-n^5}$*. Demostrar que* $\beta = \sqrt{3 + \sqrt{\alpha}}$ *es irracional.*

6.5.9. *Demostrar que todo número racional perteneciente al intervalo* $[0, 1]$ *se puede expresar como una suma finita de fracciones distintas con numerador* 1*.*

6.5.10. *Demostrar que la sucesión* $\{(n!e)\}$ *no está uniformemente distribuida.*

6.5.11. *En el primer examen saco un* $8|\sin 1|$*, en el segundo* $8|\sin 6|$*, en el tercero* $8|\sin 9|$*, y así sucesivamente. Demostrar que si el número de exámenes es suficientemente grande, la media me saldrá aprobado.*

6.5.12. *Demostrar que, dados dos enteros* a, b*,* $a \neq 0$*, la sucesión* $\{(an + b)\alpha\}$ *está uniformemente distribuida si y sólo si* α *es irracional.*

6.5.13. *Demostrar que la sucesión* $\{(\log n)\}$ *no está uniformemente distribuida.*

6.5.14. *Demostrar que la sucesión: parte fraccionaria de* $\left(\frac{\sqrt{5}+1}{2}\right)^n$ *no está uniformemente distribuida.*

6.5.15. *Demostrar que existe un* n *tal que* (ne) *tiene un* 7 *en el lugar* 77*.*

6.5.16. *Demostrar que existe un* n *tal que* $[10000(\pi n)] = 2001$*.*

6.5.17. *Calcular*

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n=1}^{x} \frac{1}{n\sqrt{3} - [n\sqrt{3}] + 1}.$$

6.5.18. *Demostrar que casi todo* x *en* $[0, 1)$ *es normal en todas las bases.*

6.5.19. *Demostrar que los números* $\alpha = 0{,}12345678910111213...$ *y* $\beta = 0{,}2357111317192329\ldots$ *son irracionales.*

6.5.20. *Sean* a, b *enteros,* $b \neq 0$*. Demostrar que* $\tan(\frac{\pi}{4}\frac{a}{b})$ *es racional si y sólo si* b *es entero.*

6.5.21. *Demostrar que si* α *es irracional entonces la sucesión* $(n^2\theta)$ *está uniformemente distribuida.*

Capítulo 7

La distribución de los números primos

En este capítulo estudiaremos la función $\pi(x)$ que cuenta el número de primos menores o iguales que x, y haremos énfasis en la fórmula asintótica

$$\pi(x) \sim \frac{x}{\log x},$$

que es conocida como "teorema de los números primos".

En el capítulo 1 vimos la formulación equivalente

$$\Psi(x) \sim x \text{ o } \lim_{x\to\infty} \frac{\Psi(x)}{x} = 1,$$

en términos de la función de Chebychev

$$\Psi(x) = \sum_{p^m \leq x} \log p = \sum_{n \leq x} \Lambda(n)$$

que resulta más conveniente porque la función Ψ tiene propiedades más sencillas de desvelar por medios analíticos.

La teoría que vamos a considerar fue esbozada por B. Riemann en una maravillosa memoria del año 1860 titulada"Ueber die Anzahl der Primzahlen unter einen gegebenen Grosse". En tan sólo ocho páginas Riemann exhibe las profundas conexiones que existen entre Ψ y la función ζ de la variable compleja $s = \sigma + i\tau$. En particular, el teorema de los números primos es una consecuencia de la no anulación de la función ζ en la línea vertical $\sigma = 1$ y fue demostrado, independientemente, por J. Hadamard y C.J, de la Vallée Poussin, más de 30 años después de la aparición del trabajo de B. Riemann.

Existe una realación explícita entre la estimación de la diferencia $\Psi(x) - x$ y los ceros de la función ζ en la banda $0 \leq \sigma \leq 1$.

Riemann formuló la hipótesis de que estos ceros estásn situados precisamente en le línea vertical $\sigma = 1/2$. Esta conjetura es uno de los problemas más famosos de las Matemáticas y posee una rica, y a veces pintoresca, historia.

A diferencia de los capítulos anteriores donde, en general no hemos necesitado más que "métodos elementales"que incolucran a lo sumo, al cálculo diferencial de una variable real, este capítulo necesita la teoría de funciones analíticas y algunas propiedades de la transformada de Fourier. Ello no debe extrañarnos, por cuanto el estudio de la distribución de los números primos fue uno de los motores que propulsó el desarrollo de la teoría de funciones y del análisis armónico, dando lugar a teorías a la vez profundas y bellas.

En torno al año 1950 A. Selberg y P. Erdős encontraron una demostración elemental de la ley asintótica, es decir, sin el recurso a la teoría de funciones analíticas. En este capítulo vamos a presentar la demostración clásica siguiendo el camino indicado por B. Riemann, y supondremos al lector familiarizado con la variable compleja.

7.0.1. La función ζ de Riemann y el Teorema de los números primos

Recordemos que Euler introdujo la función $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, definida para todo real $s > 1$ para demostrar la existencia de infinitos primos como consecuencia de la divergencia de la serie armónica $\sum_n \frac{1}{n}$.

En lo sucesivo usaremos la notación tradicional de la Teoría de los Números y designaremos con las letras σ y τ a las partes real e imaginaria, respectivamente, del número complejo s.

Siguiendo a Riemann, conviene extender el dominio de ζ al semiplano complejo $\Re(s) = \sigma > 1$, donde la serie $\sum_{n=1}^{\infty} n^{-s}$ es absolutamente convergente y define a una función analítica. En este semiplano también es cierta la identidad de Euler que conecta la sucesión de todos los enteros positivos con la de los números primos

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

La demostración es idéntica a aquella que presentamos en el capítulo 1 para s real, $s > 1$.

Tomando logaritmos en la identidad anterior y utilizando el desarrollo en serie

de Taylor de la función

$$\log(1-z) = -\sum_{m=1}^{\infty} \frac{z^m}{m},$$

valido en $|z| < 1$, obtenemos

$$\log \zeta(s) = -\sum_{p} \log\left(1 - \frac{1}{p^s}\right) = \sum_{p} \sum_{m\geq 1} \frac{1}{m} \frac{1}{p^{ms}}. \tag{7.1}$$

Si derivamos término a término la identidad anterior, obtenemos que

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{p} \sum_{m\geq 1} \frac{\log p}{p^{ms}}.$$

Recordando que la función de Mangoldt está definida por

$$\Lambda(n) = \begin{cases} \log p \text{ si } n = p^m \\ 0 \text{ en otro caso} \end{cases}$$

podemos escribir la identidad

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

7.0.2. El teorema del número primo

El teorema del número primo consiste en establecer la ley asintótica $\pi(x) \sim \dfrac{x}{\log x}$, que como vimos en el primer capítulo, es equivalente a $\Psi(x) \sim x,\ x \to \infty$.

Teorema 7.0.22 (Teorema de los números primos)**.** *$\Psi(x) \sim x$ cuando $x \to \infty$.*

Por razones que se verán más adelante conviene introducir la función primitiva

$$\Psi_1(x) = \int_0^x \Psi(t)dt.$$

Lema 7.0.23. *Si $\Psi_1(x) \sim \frac{x^2}{2}$ entonces $\Psi(x) \sim x$.*

Demostración. Dado $c > 1$, por ser $\Psi(t)$ creciente tenemos la desicualdad

$$\begin{aligned} \Psi(x) &\leq \frac{1}{(c-1)x} \int_x^{cx} \Psi(t)dt = \frac{1}{(c-1)x} \left(\Psi_1(cx) - \Psi_1(x)\right) \\ &= \frac{1}{(c-1)x} \left(\frac{(cx)^2}{2} - \frac{x^2}{2} + o(x^2)\right) = x\frac{c+1}{2} + o(x). \end{aligned}$$

Para todo $c > 1$ se tiene que

$$\limsup_{x\to\infty} \frac{\Psi(x)}{x} \leq \frac{c+1}{2},$$

y esto es cierto para todo $c > 1$. Tomando el límite cuando $c \to 1$, obtenemos finalmente que $\limsup_{x\to\infty} \frac{\Psi(x)}{x} \leq 1$. Un argumento similar, pero con $c < 1$, permite demostrar que $\liminf_{x\to\infty} \frac{\Psi(x)}{x} \geq 1$. □

Nuestro objetivo es entonces demostrar que $\lim_{x\to\infty} \frac{\Psi_1(x)}{x^2} = \frac{1}{2}$. En el lemma 7.0.25 obtendremos una formula explícita para $\Psi_1(x)$ donde aparece involucrada la función ζ. Pero antes necesitamos un lema técnico.

Lema 7.0.24. *Dados $c > 0$, $y > 0$ y $k \geq 1$ tenemos que*

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s(s+1)\cdots(s+k)}ds = \begin{cases} 0, & si\ 0 \leq y \leq 1 \\ \frac{1}{k!}\left(1-\frac{1}{y}\right)^k, & si\ y > 1. \end{cases}$$

Demostración. Es un sencillo cálculo de residuos. Consideremos la circunferencia de radio R, muy grande, centrada en el origen. La recta vertical $\sigma = c$ corta a la circunferencia en dos puntos $c \pm iT(R)$ y la divide en dos arcos, uno más grande a la izquierda al que llamaremos Γ_R^1 , y otro más pequeño a la derecha, al que llamaremos Γ_R^2. Conviene hacerse un dibujo.

Si $0 < y \leq 1$ consideramos el recinto cuya frontera es Γ_R^2 y el trozo de recta vertical $c \pm iT(R)$.

Como la función $\frac{y^s}{s(s+1)\cdots(s+k)}ds$ es analítica en ese recinto, su integral a lo largo de la frontera es cero, luego

$$\int_{c-iT(R)}^{c+iT(R)} \frac{y^s}{s(s+1)\cdots(s+k)}ds = -\int_{\Gamma_R^2} \frac{y^s}{s(s+1)\cdots(s+k)}ds.$$

Pero cuando $s \in \Gamma_R^2$ tenemos la estimación

$$\left|\frac{y^s}{s(s+1)\cdots(s+k)}\right| \leq \frac{y^c}{R(R-1)\cdots(R-k)} \ll \frac{1}{R^{k+1}}.$$

Por lo tanto

$$\left|\int_{\Gamma_R^2} \frac{y^s}{s(s+1)\cdots(s+k)}ds\right| \ll \frac{1}{R^k}$$

y

$$\int_{c-i\infty}^{c+i\infty} = \lim_{R\to\infty}\int_{c-iT(R)}^{c+iT(R)} \frac{y^s}{s(s+1)\cdots(s+k)}ds = 0.$$

Si $y > 1$ consideramos el recinto cuya frontera es Γ_R^1 y el trozo de recta vertical $c \pm iT(R)$. En este recinto, si R es suficientemente grande, la función tiene polos en $j = 0, -1, \ldots, -k$. Tenemos entonces

$$\frac{1}{2\pi i}\int_{c-iT(R)}^{c+iT(R)} \frac{y^s}{s(s+1)\cdots(s+k)}ds + \frac{1}{2\pi i}\int_{\Gamma_R^1} \frac{y^s}{s(s+1)\cdots(s+k)}ds$$
$$= \sum_{j=0}^{k} \operatorname{Res}\left(\frac{y^s}{s(s+1)\cdots(s+k)}, -j\right) = \sum_{j=0}^{k} \frac{(-1)^j y^{-j}}{j!(k-j)!} = \frac{1}{k!}\left(1-\frac{1}{y}\right)^k.$$

La demostración finaliza observando que la integral $\int_{\Gamma_R^1} \to 0$ por las mismas razones que en el caso anterior. □

Lema 7.0.25. *Para todo $c > 1$ tenemos la fórmula*

$$\frac{\Psi_1(x)}{x^2} - \frac{1}{2}\left(1-\frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right)ds.$$

Demostración. Dado $c > 1$, utilizamos el lema 7.0.24 para escribir

$$\begin{aligned}\frac{\Psi_1(x)}{x^2} = \frac{1}{x}\sum_{n\le x}\left(1-\frac{n}{x}\right)\Lambda(n) = \frac{1}{x} &= \sum_{n=1}^{\infty}\Lambda(n)\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{(x/n))^s}{s(s+1)}ds \\ &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{x^{s-1}}{s(s+1)}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}ds \\ &= \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{x^{s-1}}{s(s+1)}\left\{-\frac{\zeta'(s)}{\zeta(s)}ds\right\}ds.\end{aligned}$$

El lema 7.0.24 también nos da

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}\frac{x^{s-1}}{s(s+1)}\frac{1}{s-1}ds = \frac{1}{2}\left(1-\frac{1}{x}\right)^2.$$

Basta entonces con restar las dos identidades para demostrar el lema. Observemos que la hipótesis $\Re(s) > 1$ implica que todas las series y las integrales consideradas son absolutamente convergentes. □

Los lemas 7.0.23 y 7.0.25 nos muestran el teorema del número primo es equivalente a demostrar que para cualquier $c > 1$,

$$\lim_{x\to\infty}\int_{c-i\infty}^{c+\infty}\frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right)ds = 0.$$

Examinemos este límite. La línea de integración $s = c + i\tau, \quad -\infty < \tau < +\infty$ permite sacar el factor x^{c-1} fuera de la integral, pero $x^{c-1} \to \infty$ si $c > 1$.

Una estrategia natural consiste en trasladar la línea de integración a la línea $c = 1$. Pero para hacerlo necesitamos conocer mejor las propiedades de la función $-\dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{1}{s-1}$: analiticidad y crecimiento en un entorno de esa línea, ausencia de ceros de ζ en $1 + i\tau$, etc..

Supongamos por un momento que podemos trasladar la línea de integración a $s = 1 + i\tau$ y escribir la integral en la forma siguiente después de hacer el cambio $s = 1 + i\tau$:

$$\int_{-\infty}^{\infty} e^{i\tau \log x} h(\tau) d\tau = \hat{h}(-\log x),$$

donde

$$h(\tau) = \frac{1}{(1+i\tau)(2+i\tau)} \left\{ -\frac{\zeta'(1+i\tau)}{\zeta(1+i\tau)} - \frac{1}{i\tau} \right\}.$$

Si además demostramos que h es integrable, el Teorema de Riemann-Lebesgue nos dará entonces

$$\lim_{x \to \infty} \hat{h}(-\log x) = 0$$

y, por tanto,

$$\Psi_1(x) \sim \frac{x^2}{2}, \qquad x \to \infty.$$

En lo que resta del capítulo nos dedicaremos a probar los pasos necesarios para completar esta estrategia.

Observar primero que los posibles polos de $\frac{\zeta'(s)}{\zeta(s)}$ van a venir de los polos y de los ceros de $\zeta(s)$. En efecto, si $\zeta(s)$ tiene un polo o un cero en $s = s_0$ podemos escribir $\zeta(s) = (s - s_0)^k g(s)$ con $k \neq 0$, $g(s)$ analítica en s_0 y tal que $g(s_0) \neq 0$. Tomando logaritmos y derivando obtenemos

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{k}{s - s_0} + \frac{g'(s)}{g(s)},$$

que tiene un polo en $s = s_0$ de residuo k.

El único polo de la función ζ se analiza en el siguiente lema.

Lema 7.0.26. *La función ζ tiene una extensión al semiplano $\Re(s) > 0$, como una función meromorfa cuya única singularidad, situada en $s = 1$, es un polo simple de residuo igual a 1.*

Demostración. La fórmula de sumación de Abel nos permite escribir

$$\sum_{n\leq x}\frac{1}{n^s}=\frac{[x]}{x^s}+s\int_1^x\frac{[y]}{y^{s+1}}dy=\frac{[x]}{x^s}+s\int_1^x\frac{1}{y^s}dy-s\int_1^x\frac{\{y\}}{y^{s+1}}dy \tag{7.2}$$

$$=\frac{s}{s-1}-s\int_1^\infty\frac{\{y\}}{y^{s+1}}dy+\frac{[x]}{x^s}-\frac{sx^{-s}}{s-1}+s\int_x^\infty\frac{\{y\}}{y^{s+1}}dy \tag{7.3}$$

si $\Re(s)>1$. Y si hacemos tender x a infinito obtenemos

$$\zeta(s)=\frac{s}{s-1}-s\int_1^\infty\frac{\{y\}}{y^{s+1}}dy \tag{7.4}$$

que es una función meromorfa con un sólo polo en $s=1$ con residuo 1. □

La función ζ no va a tener ceros en la región $\sigma\geq 1$. El caso fácil $\sigma>1$ se analiza en el siguiente lema y el caso $\sigma=1$ está recogido en el apartado 4) del lema 7.0.28.

Lema 7.0.27. *Si $\sigma>1$ entonces $\zeta(s)\neq 0$.*

Demostración.

$$\frac{1}{|\zeta(s)|}=\prod_p\left|1-\frac{1}{p^s}\right|\leq\prod_p\left(1+\frac{1}{p^\sigma}\right)\leq\sum_{n=1}^\infty\frac{1}{n^\sigma}=\zeta(\sigma)<\infty. \tag{7.5}$$

□

Lema 7.0.28. *La función ζ verifica las estimaciones siguientes.*

1) En la región $\sigma\geq 1,\ |\tau|\geq 2$:

$$|\zeta(\sigma+i\tau)|\ll\log|\tau|.$$

2) En la región $1/2<1-\rho\leq\sigma<1,\ |\tau|\geq 2$:

$$|\zeta(\sigma+i\tau)|\ll\frac{|\tau|^\rho}{\rho}.$$

3) En la región $\sigma\geq 1,\ |\tau|\geq 3$:

$$|\zeta'(\sigma+i\tau)|\ll\log^2|\tau|.$$

4) Para todo τ se cumple que $\zeta(1+i\tau)\neq 0$.

5) En la región $\sigma \geq 1$, tenemos

$$\frac{1}{|\zeta(\sigma + i\tau)|} \ll \log^7 |\tau|.$$

Demostración. Observemos primero que si $\sigma > 0$ y $s \neq 1$, las fórmulas 7.2 y 7.4 nos dan la expresión

$$\zeta(s) = \sum_{n \leq x} \frac{1}{n^s} - \frac{[x]}{x^s} + \frac{s}{s-1}\frac{1}{x^{s-1}} - s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt. \tag{7.6}$$

1) Si $\sigma \geq 2$, tenemos que $|\zeta(s)| \leq \zeta(\sigma) \leq \zeta(2) = \pi^2/6$.

Si $1 \leq \sigma < 2$, los sumandos de la parte derecha de (7.6) los podemos acotar de la siguiente manera:

$$\begin{aligned}
\left|\sum_{n\leq x}\frac{1}{n^s}\right| &\leq \sum_{n\leq x}\frac{1}{n^\sigma} \leq \sum_{n\leq x}\frac{1}{n} \ll \log x \\
\left|\frac{[x]}{x^s}\right| &\leq x^{1-\sigma} \leq 1 \\
\left|\frac{s}{s-1}\frac{1}{x^{s-1}}\right| &\leq \frac{\sigma+|\tau|}{|\tau|}x^{1-\sigma} \leq \frac{2+|\tau|}{|\tau|} = \frac{2}{|\tau|} + 1 \leq 2 \\
\left|s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt\right| &\leq (\sigma+|\tau|)\int_x^\infty \frac{dt}{t^{\sigma+1}} \leq (2+|\tau|)\int_x^\infty \frac{dt}{t^2} = \frac{2+|\tau|}{x}.
\end{aligned}$$

Tomando $x = |\tau|$ obtenemos la estimación deseada.

2) En este caso las estimaciones son

$$\begin{aligned}
\left|\sum_{n\leq x}\frac{1}{n^s}\right| &\leq \sum_{n\leq x}\frac{1}{n^\sigma} \leq \sum_{n\leq x}\frac{1}{n^{1-\rho}} \ll \frac{x^\rho}{\rho} \\
\left|\frac{[x]}{x^s}\right| &\leq x^{1-\sigma} \leq x^\rho \\
\left|\frac{s}{s-1}\frac{1}{x^{s-1}}\right| &\leq \frac{\sigma+|\tau|}{|\tau|}x^{1-\sigma} \leq \frac{1+|\tau|}{|\tau|}x^\rho \leq \frac{3}{2}x^\rho \\
\left|s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt\right| &\leq (1+|\tau|)\int_x^\infty \frac{dt}{t^{2-\rho}} = (1+|\tau|)\frac{x^{\rho-1}}{1-\rho}.
\end{aligned}$$

Tomando de nuevo $x = |\tau|$ y observando que $0 < \rho < 1/2$ obtenemos la estimación.

3) Sea $s = \sigma + i\tau$ un punto situado en la región $\sigma \geq 1$, $\tau \geq 2$ y sea C un circunferencia centrada en s y con un radio $\rho < 1/2$ que fijaremos más tarde. Una

aplicación de la fórmula de Cauchy nos da

$$|\zeta'(s)| = \left| \frac{1}{2\pi i} \int_C \frac{\zeta(z)}{(z-s)^2} dz \right| \leq \frac{M}{\rho},$$

donde M es el valor máximo de $|\zeta(z)|$ en C.

Para la parte de C que está en $\Re(z) \geq 1$ utilizamos la estimación dada en 1): $\zeta(z) \ll \log|\tau|$.

Para la parte de C que está en $\Re(z) < 1$ observemos que $\Re(z) \geq \Re(s) - \rho \geq 1 - \rho$ y que $|\tau| + 1/2 \geq |\Im(z)| \geq |\Im(s)| - \rho = |\tau| - \rho \geq 2$. En este caso utilizamos la estimación dada en 2): $\zeta(z) \ll \frac{\Im(z)^\rho}{\rho} \ll \frac{|\tau|^\rho}{\rho}$.

Tomando $\rho = \frac{1}{\log|\rho|}$ obtenemos que $M \ll \log|\tau|$ y de aquí la estimación que buscábamos.

4) Comencemos con la identidad

$$3 + 4\cos\theta + \cos(2\theta) = 2(1 + \cos\theta)^2 > 0. \tag{7.7}$$

La fórmula (7.1) implica que en particular podemos escribir

$$\log\zeta(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

con $c_n = 1/m$ si $n = p^m$ y $c_n = 0$ en otro caso. En particular tenemos que $c_n \geq 0$ para todo n. Por otra parte

$$\log|\zeta(s)| = \Re(\log\zeta(s)) = \sum_{n=1}^{\infty} c_n \frac{\cos(\tau\log n)}{n^\sigma}.$$

Si aplicamos la identidad (7.7) a los tres casos $s = \sigma,\ \sigma + i\tau,\ \sigma + 2i\tau$ con $\sigma > 1$, podemos escribir:

$$\begin{aligned} 3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma + i\tau)| + \log|\zeta(\sigma + 2i\tau)| = \\ = \sum_{n=1}^{\infty} c_n \frac{3 + 4\cos(\tau\log n) + \cos(2\tau\log n)}{n^\sigma} \geq 0. \end{aligned}$$

Por tanto,

$$|\zeta(\sigma)|^3 |\zeta(\sigma + i\tau)|^4 |\zeta(\sigma + 2i\tau)| \geq 1 \tag{7.8}$$

, que es equivalente a

$$|(\sigma - 1)\zeta(\sigma)|^3 \left| \frac{\zeta(\sigma + i\tau)}{\sigma - 1} \right|^4 |\zeta(\sigma + 2i\tau)| \geq \frac{1}{\sigma - 1}.$$

Supongamos que existiese τ tal que $\zeta(1+i\tau)=0$. En ese caso $\lim_{\sigma\to 1^+}\frac{\zeta(\sigma+i\tau)}{\sigma-1}=\zeta'(1+it)$, $\lim_{\sigma\to 1^+}(\sigma-1)\zeta(\sigma)=1$ y $\lim_{\sigma\to 1^+}\zeta(\sigma+2i\tau)=\zeta(1+2i\tau)$ y llegamos a una contradicción por que $\lim_{\sigma\to 1^+}\frac{1}{\sigma-1}=\infty$.

Luego ζ no puede anularse en la recta $\sigma=1$.

5) De (7.8) obtenemos la estimación

$$\frac{1}{|\zeta(\sigma+i\tau)|}\leq|\zeta(\sigma)|^{3/4}|\zeta(\sigma+2i\tau)|^{1/4}.$$

En la región $1\leq\sigma\leq 2,\ |\tau|\geq 2$, tenemos que

$$|\zeta(\sigma)|\ll\frac{1}{\sigma-1},\qquad|\zeta(\sigma+2i\tau)|\ll\log|\tau|,$$

que sustituidas en la estimación anterior producen

$$|\zeta(\sigma+i\tau)|\geq B\frac{(\sigma-1)^{3/4}}{(\log|\tau|)^{1/4}},\qquad 1\leq\sigma\leq 2,\ |\tau|\geq 2,$$

donde $B>0$ es una constante.

Consideremos $\theta>\sigma$. Podemos escribir

$$|\zeta(\sigma+i\tau)-\zeta(\theta+i\tau)|\leq\int_\sigma^\theta|\zeta'(t+i\tau)dt\leq A(\theta-\sigma)\log^2|\tau|.$$

Esto nos da

$$|\zeta(\sigma+i\tau)|\geq|\zeta(\sigma+i\tau)|-|\zeta(\sigma+i\tau)-\zeta(\theta+i\tau)|\geq B\frac{(\sigma-1)^{3/4}}{(\log|\tau|)^{1/4}}-A(\theta-\sigma)\log^2|\tau|.$$

Finalmente escogemos $\theta=\sigma+\left(\frac{B}{2A}\right)^4\frac{1}{\log^9|\tau|}$ y al sustituir obtenemos

$$|\zeta(\sigma+i\tau)|\geq\frac{B^4}{16A^3}\frac{1}{\log^7|\tau|}.$$

□

Con el lema anterior en nuestra mano resulta muy fácil justificar el traslado de la línea vertical $c+i\tau$ con $c>1$ a la línea $1+i\tau$ en al fórmula del lema 7.0.25.

Consideremos el el contorno rectangular de lados verticales $1+i\tau,\ c+i\tau,\ |\tau|\leq T$ y lados horizontales $\sigma+iT,\ \sigma-iT,\ 1\leq\sigma\leq c$.

Los lemas 7.0.26 y 7.0.28 nos dicen que la función

$$f(s)=\frac{x^{s-1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}-\frac{1}{s-1}\right)$$

es analítica en un entorno del rectángulo R; además en los lados horizontales tenemos que

$$|f(\sigma + i\tau)| \ll x^{c-1}\frac{\log^9 T}{T^2}.$$

Es decir, fijado $x > 0$, la integral sobre los lados horizontales de la función f tiende a 0 cuando $T \to \infty$.

Por lo tanto,

$$\int_{c-i\infty}^{c+i\infty} f(s)ds = \int_{1-\infty}^{1+\infty} f(s)ds.$$

Es decir,

$$\frac{\Psi_1(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{-\infty}^{\infty} \frac{e^{i\tau \log x}}{(1+i\tau)(2+i\tau)}\left\{-\frac{\zeta'(1+i\tau)}{\zeta(1+i\tau)} - \frac{1}{i\tau}\right\} d\tau.$$

Por otra parte la función

$$h(\tau) = \frac{1}{(1+i\tau)(2+i\tau)}\left\{-\frac{\zeta'(1+i\tau)}{\zeta(1+i\tau)} - \frac{1}{i\tau}\right\} d\tau$$

verifica la acotación

$$|h(\tau)| \ll \frac{\log^9 |\tau|}{1+|\tau|^2}$$

y por lo tanto es integrable y, culminando la estrategia esbozada en la sección anterior, podemos invocar al Teorema de Riemann-Lebesgue para concluir la demostración del teorema de los números primos.