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 en *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 $a > 0$ y b, 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 $a > b > 0$ y $a = bc + r,\ 0 \leq r < b$. 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 enteros 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 $f(n) = n^2 - n + 41$ 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.

En el momento de escribir estas notas (septiembre de 2015) 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 $F_{3329780}$, que es divisible por $193 \cdot 2^{3329782} + 1$.

¿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 estimación asintótica:

$$\pi(x) \sim \frac{x}{\log x}, \tag{1.1}$$

que es equivalente a la igualdad

$$\lim_{x\to\infty} \frac{x}{x/\log x} = 1. \tag{1.2}$$

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

$$\int_m^n \frac{dx}{\log x}. \tag{1.3}$$

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 de ocho áginas 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 la 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 $0 < x \leq 1/2$ (nmirar el desarrollo de Taylor de orden 2 de la función $f(x) = \log(1-x)$) 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,

$$\sum_{p,\ p+2=p'} \frac{1}{p} < +\infty, \tag{1.4}$$

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

1.2.2. El teorema de Chebychev

En una memoria publicada en el año 1859 Chebychev demostró que el orden de magnitud de $\pi(x)$ era el pronosticado. En su estudio introdujo las funciones $\Theta(x)$ y $\Psi(x)$ definidas para todo número real positivo por medio de las fórmulas:

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

donde la suma está tomada sobre todos los primos p menores o iguales que x, y

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

donde en este caso las suma está extendida sobre todas las potencias de primos menores o iguales que x. En lo sucesivo la letra p designará siempre a un primo.

Si en la fórmula que define a $\Psi(x)$ agrupamos los términos para los cuales m tiene el mismo valor, obtenemos

$$\Psi(x) = \Theta(x) + \Theta(x^{1/2}) + \Theta(x^{1/3}) + \cdots$$

La serie que aparece en el segundo miembro de la igualdad anterior contiene sólo un número finito de términos distintos de cero, puesto que $\Theta(y) = 0$ cuando $y < 2$.

Por otro lado, en la suma que define a $\Psi(x)$, cada $\log p$ aparecerá tantas veces como enteros positivos m satisfagan $p^m \leq x$. Tomando logaritmos, $m \leq \log x / \log p$. Entonces

$$\Psi(x) = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \tag{1.5}$$

donde para cada número real $r > 0$, $\lfloor r \rfloor$ designa al mayor entero no negativo que es menor o igual que r. El entero $\lfloor r \rfloor$ se llama parte entera de r, mientras que el número real $\{r\} = r - \lfloor r \rfloor$ se conoce como parte fraccionaria de r.

Teorema 1.2.3. *Los tres cocientes*

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

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

Demostración. Sean

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

Tenemos que

$$\Theta(x) \leq \Psi(x) \leq \sum_{p \leq x} \frac{\log x}{\log p} \log p = \pi(x) \log x.$$

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

Por otro lado, si $x > 1$ y elegimos un número $\alpha,\ 0 < \alpha < 1$, tenemos que

$$\Theta(x) \geq \sum_{x^\alpha < p \leq x} \log p \geq \log(x^\alpha)(\pi(x) - \pi(x^\alpha)).$$

Y como $\pi(x^\alpha) \leq x^\alpha$, obtenemos la relación

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

Tomando límites superiores y teniendo en cuenta que $\log x/x^{1-\alpha}$ tiende a cero, deducimos que $A_2 \geq \alpha A_1$. Pero como esta desigualdad es válida para cada $\alpha,\ 0 < \alpha < 1$, tenemos que $A_2 \geq A_1$. Por tanto $A_1 = A_2 = A_3$. La identidad $a_1 = a_2 = a_3$ se demuestra de manera análoga. □

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 1.2.4. *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 1.2.5 (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 1.2.6. *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 1.2.7 (Chebychev)**.** *Para todo $x\geq 2$ se tiene que*

$$\frac{x}{4\log x} \leq \pi(x) \leq \frac{4x}{\log x}. \tag{1.6}$$

Demostración. Se puede comprobar a mano que el Teorema es cierto para $x<25$. Suponemos pues que $x\geq 25$.

Separando los primos menores que $\sqrt{n}$ en el Lema 1.2.4 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 $\pi(\sqrt{n}) \leq \sqrt{n}$ y que $2\log 4 + \frac{\log n}{\sqrt{n}} \leq 4$ para $n \geq 25$, vemos que

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

Si x es real tenemos

$$\pi(x) = \pi(\lfloor x \rfloor) \leq 4\frac{\lfloor x \rfloor}{\log \lfloor x \rfloor} \leq 4\frac{x}{\log x}$$

debido a que la funcin $t/\log t$ es creciente para $t > e$.

Para la cota inferior observemos primero que $\binom{2n}{n} = \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1} > 2^n$. El corolario 1.2.6 nos permite deducir que

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

Tomando logaritmos,

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

En particular, para cualquier x real se obtiene

$$\pi(x) \geq \pi(2\lfloor x/2 \rfloor) \geq \frac{(\log 2)\lfloor x/2 \rfloor}{\log(2\lfloor x/2 \rfloor)} \geq \frac{(\log 2)(x/2-1)}{\log x} = \frac{x}{\log x}\left(\frac{\log 2}{2} - \frac{(\log 2)(\log x)}{x}\right).$$

La demostración finaliza observando que la cantidad entre paréntesis es mayor que $1/4$ para $x \geq 25$. □

Teorema 1.2.8 (Postulado de Bertrand)**.** *Para todo $n > 1$ existe un número primo p tal que $n < p < 2n$.*

Demostración. 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,

$$\frac{4^n}{2n+1} \leq \binom{2n}{n}.$$

Continuemos 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 1.2.6 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 1.2.6 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 $n \geq 520$. 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. □

1.3. Resultados recientes sobre los números primos

Los últimos años han sido especialmente fructíferos en el estudio de los números primos. Estos son algunos ejemplos.

1.3.1. Primos en progresión aritmética y cuadrados mágicos

Una conjetura clásica acerca de los números primos afirmaba que la sucesión de los números primos contenía progresiones aritméticas arbitrariamente largas. Esta conjetura fue demostrado finalmente por B. Green y T. Tao en 1998.

Teorema 1.3.1 (B. Green, T. Tao, 1998)**.** *Para todo $k \geq 3$ existen k primos en progresión aritmética.*

De hecho posteriormente desarrollaron técnicas más sofisticadas que les permitieron hallar el comportamiento asintótico del número de soluciones en números

primos de algunos sistemas de ecuaciones. Utilizando esta maquinaria, Carlos Vinuesa, que fue estudiante de la UAM, halló una fórmula asintótica para el número de cuadrados mágicos 3×3 formados por números primos menores o iguales que x.

Teorema 1.3.2 (Carlos Vinuesa, 2012)**.** *Si $M(x)$ es el número de cuadrados mágicos de orden 3×3 formado por números primos menores o iguales que x, se tiene que*

$$M(x) \sim c\frac{x^3}{\log^9 x}$$

donde c es una constante explícita.

1.3.2. El problema ternario de Goldbach

En su carta a Euler, Goldbach afirmaba haber observado que todo entero par mayor que 2 era suma de dos primos y que todo impar mayor que 5 era suma de tres primos. La primera de ellas es conocida como la conjetura de Goldbach o el problema binario de Goldbach y se cree que los métodos actuales son insuficientes para resolverla. La segunda de ellas es conocida como el problema ternario de Goldbach. Vinogradov dio una respuesta bastante satisfactoria demostrando que todo impar mayor que una cierta constante C se puede escribir como suma de tres primos. Pero hasta hace muy poco esa constante C era tan grande que resultaba impracticable comprobar la conjetura para todos los impares menores que C, incluso utilizando la potencia de todos los ordenadores del mundo simultaneamente y durante todos los años que durase nuestro planeta.

Pero Harald Helfgott, un matemático peruano que ha visitado nuestro Departamento en varias ocasiones, hizo unas mejoras teóricas que permitieron reducir dicha constante C hasta $C = 10^{30}$ (anteriormente estaba en 10^{300}). Hasta esa cantidad sí que era factible comprobarlo y Harald lo hizo en menos de tres meses con ayuda de potentes ordenadores.

Teorema 1.3.3 (Harald Helfgott, 2013)**.** *Todo impar mayor que* 5 *se puede escribir como suma de tres primos.*

1.3.3. Lagunas entre primos y los primos gemelos

La conjetura de los primos gemelos dice que $p_{n+1} - p_n = 2$ para infinitos n. Es fácil demostrar que el teorema de los números primos implica que $\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log n} \leq 1$. Erdős demostró que la desigualdad era estricta y posteriormente la constante 1 fue sustituyéndose por constantes cada vez más pequeñas pero positivas. Esto fue así hasta que Goldston, Pintz y Yildirim demostraron en 2006 que $\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log n} =$

0. De hecho demostraron que $p_{n+1}-p_n \leq \sqrt{\log n}$ para infinitos n. Esto fue considerado un gran avance en el problema de los primos gemelos pero sólo era el preludio de algo mucho má espectacular. Yitang Zhang, un matemático estadounidense prácticamente desconocido introdujo una idea nueva que le permitió demostrar una versión débil del problema de los primos gemelos.

Teorema 1.3.4 (Y. Zhang, 2013)**.** *Para infinitos n se tiene que*

$$p_{n+1} - p_n \leq 70000000.$$

En 2014, Marynard, un joven matemático, introdujo ideas adicionales que le permitieron bajar la constante hasta 600 y además demostrar que

$$H_m = \liminf_{n\to\infty}(p_{n+m} - p_n) < \infty$$

para todo $m \geq 1$. El esfuerzo de muchos otros matemáticos ha permitido llegar a la cota $H_1 \leq 246$.

1.3.4. El mínimo común múltiplo de los n primeros valores de un polinomio

Es un ejercicio sencillo comprobar que

$$\Psi(n) = \log \text{m.c.m}(1, \ldots, n).$$

Así que el teorema de los números primos es equivalente a la fórmula asintótica

$$\log \text{m.c.m}(1, \ldots, n) \sim n.$$

Batemann demostró, utilizando el teorema del número primo en progresiones aritméticas, que si $f(x) = a + bx$ con $(a, b) = 1$ entonces

$$\log \text{m.c.m.}(f(1), \ldots, f(n) \sim Cn$$

donde C es una constante que depende sólo de b.

En 2011, el que escribe estas notas halló un resultado análogo para polinomios cuadráticos. Cuando $f(x)$ es un polinomio cuadrático reducible, el comporamiento asintótico es lineal en n y sencillo de estudiar. El caso difícil aparece cuando $f(x)$ es irreducible.

Teorema 1.3.5 (J. Cilleruelo, 2011)**.** *Sea $f(x)$ un polinomio cuadrático irreducible con coeficientes enteros. Se tiene que*

$$\log m.c.m.(f(1), \ldots, f(n)) = n \log n + Bn + o(n)$$

donde B es una constante que depende de f.

En el caso más sencillo $f(x) = x^2 + 1$, el valor de la constante del teorema anterior es

$$B = \gamma - 1 - \frac{\log 2}{2} - \sum_{p \neq 2} \frac{(-1)^{\frac{p-1}{2}} \log p}{p-1} = -0{,}066275634213060706383..$$

Se conjetura que si $f(x)$ es irreducible de grado $r \geq 2$ entonces

$$\log \text{m.c.m.}(f(1), \ldots, f(n)) \sim (r-1)n \log n,$$

pero sólo se sabe cierto para $r = 2$.

1.4. Ejercicios del capítulo 1

1.4.1. *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.*

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

¿Qué edades tenían las hijas de D. Pedro?

1.4.2. *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?*

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

1.4.4. *Un cuadrado de* $n \times n$ *números enteros se dice que es un cuadrado mágico multiplicativo si el producto 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 todos los cuadrado mágicos multiplicativos* 3×3 *donde el número central es 15 y los nueve enteros positivos que forman el cuadrado son distintos.*

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

1.4.6. *Demostrar que en cualquier conjunto de* $n + 1$ *enteros positivos menores o iguales que* $2n$ *siempre hay uno que divide a otro.*

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

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

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

1.4.10. *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.

1.4.11. *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 $\pi(x) \geq \log_2 \log_2 x - 1$, $x \geq 2$.*

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

1.4.13. *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.*

1.4.14. *Demostrar que para todo $\alpha > 0$ y para todo $\epsilon > 0$, existen enteros positivos a, b tales que $|\frac{a}{b} - \alpha| < \epsilon$ y $a + b$ es primo.*

1.4.15. *Demostrar que*

i) si $2^n + 1$ es primo, entonces n es cero o una potencia de 2.

ii) si $2^n - 1$ es primo, entonces n tiene que ser primo.

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

1.4.17. *Demostrar que un polinomio $P(n)$ con coeficientes enteros no puede ser primo para todo $n \geq n_0$, sea quien sea n_0.*

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

1.4.19. *Demostrar que el Teorema de los números primos implica que*

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log n} \leq 1.$$

1.4.20. *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.*

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

1.4.22. *Demostrar que para todo $x \geq 3$ se tiene que*

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

1.4.23. *Sea $s > 1$. Demostrar que*

$$\zeta(s) = \zeta(2s) \prod_{p} \left(1 + \frac{1}{p^s}\right).$$

Utilizar esta identidad y la desigualdad $\log(1+t) \leq t$ para $t \geq 0$, para demostrar que la suma de los inversos de los primos es infinita.

1.4.24. *Utilizar el Teorema de Chebychev para 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. Demostrar también que la estimación asintótica $p_n \sim n\log n$ es equivalente al Teorema de los Números Primos.

1.4.25. *Demostrar que*

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

1.4.26. *Demostrar que*

$$m.c.m.(1, 2, \ldots, n) = e^{\Psi(n)}.$$

Deducir que la expresión

$$e^{\Psi(2N+1)} \int_0^1 x^N (1-x)^N dx$$

representa un entero positivo y utilizar este hecho para demostrar que $\Psi(2N+1) \geq N\log 4$.

1.4.27. *Sabiendo que para $(a, q) = 1$ se tiene que*

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \log p \sim \frac{x}{\phi(q)},$$

hallar una estimación asintótica para

$$\log m.c.m.(a+q, a+2q, \ldots, a+nq).$$