Divisibilidad

Mario Pineda Ruelas
Departamento de Matemáticas,
Universidad Autónoma Metropolitana-Iztapalapa
correo electrónico: mpr@xanum.uam.mx

Gabriel D. Villa Salvador
Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados, IPN
correo electrónico gvilla@ctrl.cinvestav.mx

1 Inducción matemática

En este trabajo $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ denotan a los números naturales, enteros, racionales, reales y complejos respectivamente. Por principio, no consideramos al número 0 como número natural y escribiremos $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Esto es todo lo que necesitamos para empezar nuestro estudio de la aritmética de $\mathbb{Z}$.

La esencia de las matemáticas se encuentra en la construcción de *pruebas* de afirmaciones generales por medio de argumentos lógicos. Por supuesto que el realizar éstas construcciones puede requerir de gran talento. Afortunadamente, existen métodos elementales y poderosos que sirven para llevar a cabo éstas construcciones, es decir, sirven para hacer demostraciones matemáticas.

Nuestro primer objetivo es explorar dos de los métodos más importantes en la matemática que son usados para hacer demostraciones. Estos son: el *Principio de Inducción Matemática* (**PI**) y su equivalente, el *Principio del Buen Orden* (**PBO**). Concretamente, estos dos métodos establecen lo siguiente:

Principio de Inducción Matemática: Sea S un subconjunto de $\mathbb{N}$ tal que:

(1) $1 \in S$, y

(2) Si los enteros $1, ..., n \in S$, se tiene que $n + 1 \in S$.

Entonces $S = \mathbb{N}$.

Principio del Buen Orden: Cualquier subconjunto $S \neq \emptyset$ de $\mathbb{N}$ contiene un elemento m que satisface $m \leq x$ para todo elemento $x \in S$.

Una observación simple en el Principio del Buen Orden es que el entero m es único. En el siguiente resultado vamos a suponer que $\mathbb{N}$ está dotado del orden natural $\leq$ y usaremos que el 1 no es el sucesor de ningún otro número natural. Ésta última propiedad en realidad es uno de los axiomas de Peano.

Teorema 1.1. *El Principio del Buen Orden es equivalente al Principio de Inducción Matemática.*

Demostración: Sea S un conjunto que satisface (1) y (2) del Principio de Inducción y S^c su complemento con respecto a $\mathbb{N}$. Vamos a suponer que el **PBO** se cumple. Si $S^c \neq \emptyset$, entonces existe $m \in S^c$ tal que $m \leq n$, para todo $n \in S^c$ y $m \neq 1$. Observemos en particular que $m - 1 \notin S^c$ pues m es el menor elemento de S^c. Por lo tanto $m - 1 + 1 = m \in S$. Esto último no es posible pues $m \in S^c$. Así, $S^c = \emptyset$ y $S = \mathbb{N}$.

Ahora supongamos el **PI** válido y sea S un subconjunto no vacío de $\mathbb{N}$. Vamos a suponer que el conjunto S no contiene un elemento m tal que $m \leq x$ para todo $x \in S$. Es claro que $1 \notin S$ pues de lo contrario S tendría un elemento menor. Sea $C = \{n \in \mathbb{N} : n < x, \text{ para cualquier } x \in S\}$. Es claro que $1 \in C$ pues $1 < x$ para todo $x \in S$. Mostraremos que si $k \in C$, entonces $k + 1 \in C$ y luego usaremos el **PI** para concluir que $C = \mathbb{N}$. Si $k \in C$ y $k + 1 \notin C$, entonces para algún $x_1 \in S$ se tiene $x_1 \leq k + 1$. Puesto que S no tiene un elemento mínimo, existe $x_2 \in S$ tal que $x_2 < x_1 \leq k + 1$. Así que $x_2 < k + 1$ y en consecuencia $x_2 \leq k$. Esto último no es posible pues $k < x_2$. Este absurdo nace de suponer que $k + 1 \notin C$. Por lo tanto $k + 1 \in C$ y por el **PI** tenemos que $C = \mathbb{N}$. Particularmente, si $x \in S$, se tiene que $x \in C$. Esto significa que $x < x$, lo cual no es posible. Por lo tanto, S debe contener un elemento m tal que $m \leq x$ para todo $x \in S$.

□

Nota importante: En el conjunto $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ también se cumple el **PBO**. Es muy fácil entender esto. Recordemos que la relación $\leq$ define en $\mathbb{N}$ un *orden parcial* (es reflexivo, antisimétrico y transitivo) que además satisface la ley de tricotomía (orden parcial + tricotomía=*orden total*). Este orden total resulta ser un *buen orden* porque satisface el **PBO**. Para $\mathbb{N}_0$ aprovechamos el orden total de $\mathbb{N}$ simplemente extendiéndolo, i.e, definimos $0 < j$ para $j \in \mathbb{N}$. Así tenemos un orden total en $\mathbb{N}_0$ que satisface la ley de tricotomía. Es claro que cualquier subconjunto $S \neq \emptyset$ de $\mathbb{N}_0$ contiene un elemento menor. Nos preguntamos ahora cómo queda el correspondiente principio de inducción. Muy sencillo: Si S es un subconjunto no vacío de $\mathbb{N}_0$ que satisface las propiedades:

(1) $0 \in S$.

(2) Si los enteros $0, 1, ..., n \in S$ implica que $n + 1 \in S$,

entonces $S = \mathbb{N}_0$. En general tenemos:

Proposición 1.2. *Sea X un conjunto finito de objetos y $\mathbb{N}_X = \mathbb{N} \cup X$. Si $\mathbb{N}_X$ tiene un orden total que restringido a $\mathbb{N}$ coincide con el orden $\leq$, entonces cualquier $S \subseteq \mathbb{N}_X$ no vacío contiene un elemento menor.*

Demostración: Si $X = \{x_1, x_2, ..., x_r\}$, definimos $x_i < x_j$ si $i < j$ y $x_i < n$ para $n \in \mathbb{N}$. Este es un orden total en S_X que satisface el **PBO**.

□

¿Cómo queda el correspondiente principio de inducción?

Una aplicación del principio de inducción y bastante útil en casi toda la matemática es el binomio de Newton. Observemos los siguientes expresiones:

$$\begin{aligned}(x+y)^2 &= x^2 + 2xy + y^2,\\ (x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3,\\ (x+y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.\end{aligned}$$

En cada caso, los exponentes de x y y respetan una *regla*: mientras el exponente de x va disminuyendo, el exponente de y aumenta, empezando uno en $2, 3$ ó 4 y terminando el otro $2, 3$ ó 4 respectivamente. Seguramente este comportamiento es fácil de recordar. Sin embargo, a simple vista, no podemos identificar si los coeficientes que aparecen en cada expresión, respetan alguna regla.

Definición 1.3. *Para $n \in \mathbb{N}$, el factorial de n es $n! = n(n-1)(n-2)\cdots 2$ y si $n = 0$, entonces definimos $0! = 1$.*

De algún principio fundamental del conteo sabemos que si tenemos un conjunto X con n elementos y $r \leq n$, entonces el número de subconjuntos de X con r elementos se calcula por medio de la fórmula

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

El símbolo $\binom{n}{r}$ se conoce como *coeficiente binomial* y satisface al menos las siguientes fórmulas:

Lema 1.4. *Sea $n \in \mathbb{N}$ y j un entero ≥ 0. Entonces*

1. $\binom{n}{0} = \binom{n}{n} = 1.$
2. $\binom{n}{j-1} + \binom{n}{j} = \binom{n+1}{j}.$

Demostración: Sólo demostraremos la parte 2.

$$\binom{n}{j-1} + \binom{n}{j} = \frac{n!}{(n-(j-1))!(j-1)!} + \frac{n!}{(n-j)!j!}$$

$$= \frac{n!}{(n-(j-1))!j!}(j+n-(j-1)) = \frac{(n+1)!}{(n+1-j)!j!} = \binom{n+1}{j}.$$

Podemos notar ahora que

$$\begin{aligned}
(x+y)^2 &= \binom{2}{0}x^2 + \binom{2}{1}xy + \binom{2}{2}y^2,\\
(x+y)^3 &= \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3,\\
(x+y)^4 &= \binom{4}{0}x^4 + \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 + \binom{4}{3}xy^3 + \binom{4}{4}y^4.
\end{aligned}$$

Nuestra primera aplicación del principio de inducción es el célebre Teorema del Binomio de Newton.

Teorema 1.5. *Sean $x, y \in \mathbb{R}$ y $n \in \mathbb{N}$. Entonces*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Demostración: Si $n = 1$, el resultado es evidente. Supongamos que

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Entonces

$$\begin{gathered}
(x+y)^{n+1} = (x+y)(x+y)^n =\\
(x+y)\Big[\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\Big] =\\
\binom{n}{0}x^{n+1} + \binom{n}{1}x^n y + \binom{n}{2}x^{n-1}y^2 + \cdots + \binom{n}{n-1}x^2y^{n-1} + \binom{n}{n}xy^n) + \cdots +\\
\binom{n}{0}x^n y + \binom{n}{1}x^{n-1}y^2 + \cdots + \binom{n}{n-1}xy^n + \binom{n}{n}y^{n+1} =\\
\binom{n}{0}x^{n+1} + \Big[\binom{n}{1} + \binom{n}{0}\Big]x^n y + \Big[\binom{n}{2} + \binom{n}{1}\Big]x^{n-1}y^2 + \cdots +\\
\Big[\binom{n}{n-1} + \binom{n}{n}\Big]xy^n + \binom{n}{n} =\\
\binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n y + \cdots + \binom{n+1}{n}xy^n + \binom{n+1}{n+1}y^{n+1}.
\end{gathered}$$

Notemos que al final estamos utilizando la segunda parte del Lema 1.4.

□

2 Divisibilidad

En esta sección, nuestro primer tema de estudio es el célebre *algoritmo de la división*, el cual es propiamente un proceso de aproximación por medio de múltiplos de un entero. En la sección 5.4 del Capítulo 5 veremos la importancia de extender éste algoritmo a otros *enteros*, dando como resultado la posibilidad de extraer propiedades similares a las de los enteros ordinarios. El primer testimonio escrito del algoritmo de la división se encuentra en el libro FULANO de "Los Elementos" de Euclides [1].

Teorema 2.1. [Algoritmo de la división] *Sean* $a, b, \in \mathbb{Z}$ *con* $a \neq 0$. *Existen enteros* q *y* r *únicos tal que* $b = aq + r$ *donde* $0 \leq r < |a|$.

Demostración: Primero mostraremos que la expresión de b en la forma requerida, existe. Consideremos el conjunto

$$S = \{b - am : m \in \mathbb{Z}\}.$$

Es claro que $S \cap \mathbb{N} \neq \emptyset$. Si $S_0 = S \cap \mathbb{N}_0$, entonces por el **PBO**, S_0 contiene un elemento r que satisface $r \leq n$ para todo $n \in S_0$. Lo anterior nos asegura que $0 \leq r = b - aq$ para algún $q \in \mathbb{Z}$. Veamos que $r < |a|$. Puesto que $a \neq 0$, tenemos $a \geq 1$ ó $a \leq -1$. Si $a \geq 1$ entonces

$$b - a(q + 1) = b - aq - a < b - aq = r,$$

así que

$$r - a = b - a(q + 1) < 0,$$

y por lo tanto $r < a$. El caso $a \leq -1$ se sigue al considerar que $b - a(q - 1) < 0$. Cualquiera que sea el caso, $r < |a|$.

Finalmente probaremos la unicidad de q y r. Supongamos que

$$b = aq_1 + r_1 = aq_2 + r_2,$$

con

$$0 \leq r_1 < |a| \qquad \text{y} \qquad 0 \leq r_2 < |a|.$$

Notemos que la igualdad $a(q_1 - q_2) = r_2 - r_1$ implica que $r_2 - r_1$ es un múltiplo de a y puesto que

$$-|a| < r_2 - r_1 < |a|,$$

entonces necesariamente $r_2 - r_1 = 0$ y por lo tanto $q_2 = q_1$.

□

Usaremos el algoritmo de la división para obtener un importante resultado sobre la representación de números naturales.

[1] Fundador de la escuela de matemáticas de la Universidad de Alejandría. Recibió probablemente su formación matemática en la Academia Platónica de Atenas; desgraciadamente poco se sabe de su vida. Algunos historiadores lo ubican 300 a.c. Su obra más sobresaliente es *Los Elementos* el cual es resultado de una recopilación sistemática de trabajos anteriores sobre geometría, teoría de números y álgebra elemental. Se sabe que Euclides fue un hombre de notable amabilidad y modestia, con un gran talento en el ejercicio del magisterio.

Corolario 2.2. *Sea $a \in \mathbb{N}$ con $a > 1$. Entonces cualquier entero $x > 0$ tiene una expresión única de la forma $x = b_0 + b_1 a + \cdots + b_n a^n$ con $n \geq 0$, $0 < b_n < a$ y $0 \leq b_i < a$ para $0 \leq i \leq n-1$.*

Demostración: La existencia de tal expresión la justificaremos aplicando inducción sobre x.
Si $x = 1$ el resultado es evidente. Supongamos que cualquier entero positivo $m < x$ puede ser representado de manera única en la forma

$$r_0 + r_1 a + ... + r_{k-1} a^{k-1} + r_k a^k,$$

donde

$$0 \leq r_i < a, \qquad 0 \leq i \leq k \qquad \text{y} \qquad r_k > 0.$$

Por el algoritmo de la división $x = qa + r$, $0 \leq r < a$. Si $q = 0$, entonces $x = r$ es la representación que buscamos. Si $q = x$ entonces $r = 0$, $a = 1$ es imposible pues por hipótesis $a > 1$. El caso $q > x$ no es posible por el Teorema 2.1. Por lo anterior podemos suponer que $0 < q < x$.

Por hipótesis de inducción tenemos que

$$q = r_0 + r_1 a + ... + r_{k-1} a^{k-1} + r_k a^k,$$

con $0 \leq r_i < a$ y $r_k > 0$. Entonces

$$x = aq + r = r_k a^{k+1} + r_{k-1} a^k + \ldots + r_1 a^2 + r_0 a + r,$$

y con un cambio de índices apropiado obtenemos

$$x = b_0 + b_1 a + \ldots + b_n a^n.$$

Por último mostraremos la unicidad de esta representación. Si tenemos las representaciones

$$x = b_0 + b_1 a + \ldots + b_n a^n = c_0 + c_1 a + \ldots + c_j a^j$$

tenemos que

$$0 = h_0 + h_1 a + \ldots + h_s a^s,$$

con $|h_i| < a$ para $0 \leq i \leq s$, $\quad h_i = c_i - b_i$, $\quad h_s \neq 0$, $\quad s \geq 0$.

Puesto que $|h_i| < a$, entonces $h_i \leq a - 1$ y así

$$a^s \leq |h_s a^s| = |h_0 + h_1 a + \ldots + h_{s-1} a^{s-1}| \leq$$

$$|h_0| + |h_1| a + \ldots + |h_{s-1}| a^{s-1} \leq$$

$$(a-1) + (a-1)a + ... + (a-1)a^{s-1} =$$

$$(a-1)(1 + a + ... + a^{s-1}) = a^s - 1,$$

lo cual es absurdo.

□

Definición 2.3. *Si $x \in \mathbb{R}$, denotamos por $[x]$ al mayor entero menor o igual a x.*

Algunas propiedades elementales de la función $[x]$.

Lema 2.4. *La función $[x]$ satisface:*

1. *Para $x \in \mathbb{R}$ se tiene $[x] - 1 \leq x - 1 < [x] \leq x$.*
2. *$[x + n] = n + [x]$ para cualquier $n \in \mathbb{Z}$.*
3. *Si $x, y \in \mathbb{R}$, entonces $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$.*

Demostración: Para la afirmación 1 tenemos $[x] \leq x < [x] + 1$. Por lo tanto $[x] - 1 \leq x - 1 < [x] \leq x$. Para la afirmación 2 tenemos

$$n + [x] - 1 < n + [x] \leq n + x.$$

La afirmación 3 se queda como ejercicio para el lector.

□

El siguiente resultado es de gran utilidad pues nos dice cómo encontrar q en el algoritmo de la división.

Teorema 2.5. *Sean $a, b \in \mathbb{Z}$ como en el algoritmo de la división. Si $a \geq 1$, entonces $q = \left[\frac{b}{a}\right]$. Si $a \leq -1$ y $r = 0$, $q = \left[\frac{b}{a}\right]$. Si $a \leq -1$ y $r > 0$, $q = \left[\frac{b}{a}\right] + 1$.*

Demostración: Si $a \geq 1$ se tiene que

$$aq \leq aq + r = b < aq + a = a(q + 1).$$

De esta forma obtenemos

$$q \leq \frac{b}{a} < q + 1,$$

y por lo tanto $q = \left[\frac{b}{a}\right]$. Si $a \leq -1$ y $r = 0$, entonces $\frac{b}{a} = q$ y $q = \left[\frac{b}{a}\right]$.

Por último, supongamos que $a \leq -1$ y $r > 0$. En este caso $-1 < \frac{r}{a} < 0$. De lo anterior obtenemos

$$q - 1 < q + \frac{r}{a} = \frac{b}{a} < q,$$

y por lo tanto $\left[\frac{b}{a}\right] + 1 = q$.

□

Definición 2.6. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$, $b = aq + r$, $0 \leq r < |a|$ como en el algoritmo de la división. Si $r = 0$, entonces diremos que a divide a b. También es usual decir que b es múltiplo de a o que a es un divisor de b.*

La definición de divisibilidad depende del sistema algebraico que se use. Por ejemplo, en el campo $\mathbb{Q}$ tenemos que 7 divide a 6. Es obvio que 7 no divide a 6 en $\mathbb{Z}$. Por lo tanto, la noción de divisibilidad depende no sólo de los elementos a, b que se elijan, sino que también depende de la estructura algebraica en la cual se esté trabajando. Escribiremos $a \mid b$ si a divide a b y $a \nmid b$ en caso contrario.

El siguiente resultado sintetiza las propiedades más importantes de la divisibilidad.

Teorema 2.7. *Sean $a, b, c \in \mathbb{Z}$. Se tiene que:*

1. *Si $a \neq 0$, entonces $a \mid 0$, $1 \mid a$, $a \mid a$.*
2. *Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
3. *Si $a \mid x_1$, $a \mid x_2, \ldots, a \mid x_n$, entonces $a \mid \sum_{i=1}^{n} \alpha_i x_i$ para todo $\alpha_i \in \mathbb{Z}$.*
4. *Si $b \neq 0$ y $a \mid b$, entonces $|a| \leq |b|$.*
5. *Si $a \mid b$ y $b \mid a$, entonces $|a| = |b|$.*
6. *Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.*

Demostración: Dejamos al lector la demostración de este teorema y sólo justificaremos la propiedad 4. Si $b \neq 0$ y $a \mid b$ entonces $b = aq$. Por tanto $|b| = |a||q|$. Pero $b \neq 0$ implica que $|q| \geq 1$, lo cual quiere decir que $|a| \leq |a||q| = |b|$, es decir, $-|b| \leq a \leq |b|$.

□

La importancia de la parte 4 del teorema anterior es que cualquier entero $\neq 0$ sólo admite un número finito de divisores. Este hecho es muy importante porque, entre otras cosas, nos justifica la existencia del máximo común divisor de dos enteros.

3 Máximo común divisor

Sea $D(a) = \{c \in \mathbb{N} : c \mid a\}$ el conjunto de divisores positivos de a. Es claro que este conjunto no es vacío y para $b \in \mathbb{Z}$ se tiene que $D(a) \cap D(b)$ es el conjunto de divisores positivos en común de los enteros a y b. Se puede mostrar fácilmente que si $a \neq 0$ o $b \neq 0$, entonces $D(a) \cap D(b)$ es un conjunto finito.

Definición 3.1. *sean $a, b \in \mathbb{Z}$ con a ó $b \neq 0$. Definimos el máximo común divisor(*mcd*) de a y b como el divisor en común positivo más grande de a y b.*

Observemos que el mcd de a y b existe porque $D(a) \cap D(b)$ es un conjunto finito. Denotamos $\text{mcd}(a, b)$ al mcd de a y b. ¿Qué tal si $a = b = 0$?

Definición 3.2. *Si $\text{mcd}(a, b) = 1$ diremos que a y b son primos relativos.*

Como ejemplo a la definición de mcd tenemos que 18 y -42 tienen como divisores en común a $\pm 1, \pm 2, \pm 3, \pm 6$. Por tanto $\text{mcd}(18, -42) = 6$. Notemos que los divisores en común de 18 y -42 dividen a $6 = \text{mcd}(18, -42)$. Demostraremos que esto no es una simple casualidad, es decir, este hecho es la propiedad que caracteriza al mcd.

Teorema 3.3. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0 \neq b$.*

1. *Existen $x_0, y_0 \in \mathbb{Z}$ tal que $\text{mcd}(a, b) = ax_0 + by_0$.*
2. *Sea $g = \text{mcd}(a, b)$ y $c \in \mathbb{Z}$. Entonces $c \mid a$ y $c \mid b$ si y sólo si $c \mid g$.*

Demostración: 1. Sea $g = \text{mcd}(a, b)$. Consideremos el conjunto

$$S = \{ax + by : x, y \in \mathbb{Z} \setminus \{0\}\}.$$

Tomando $x = \pm 1, y = 0$ vemos que $S \cap \mathbb{N} \neq \emptyset$. Si $S_0 = S \cap \mathbb{N}$, entonces por el **PBO**, existen $x_0, y_0 \in \mathbb{Z}$ tales que $d = ax_0 + by_0$ es el menor entero positivo en S_0. Si $d \nmid a$, entonces por el algoritmo de la división $a = dq + r$ y $0 < r < d$. Así que

$$r = a - dq = a - q(ax_0 + by_0) = a - qax_0 - qby_0 = a(1 - qx_0) + b(-qy_0).$$

Por tanto $r \in S_0$, lo cual es absurdo y $d \mid a$. Similarmente $d \mid b$. Por lo tanto $d \leq g$. Por último, $a = ga_0,\ b = gb_0$ implica que $g \mid ax_o$ y $g \mid by_0$. Así que $g \mid d$ y obtenemos la igualdad entre g y d.

La parte 2 es inmediata.

□

En la prueba anterior de paso obtuvimos que $\text{mcd}(a, b)$ es la mínima combinación lineal positiva de los enteros a y b. Notemos que los enteros x_0, y_0 no necesariamente son únicos, por ejemplo:

$$8 = \text{mcd}(-24, 8) = -24(0) + 8(1) = -24(1) + 8(4).$$

Corolario 3.4. *Si* $\mcd(a,b) = g$*, entonces* $\mcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

Demostración: Escribimos $g = ax_0 + by_0$. Observemos que los números $\frac{a}{g}$ y $\frac{b}{g}$ son enteros. Por lo tanto $1 = \frac{a}{g}x_0 + \frac{b}{g}y_0$ y $\mcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

□

Corolario 3.5. $\mcd(a,b) = 1$ *si y sólo si la ecuación* $ax + by = 1$ *es soluble en* $\mathbb{Z}$.

□

Corolario 3.6. *Sean* $a_1, a_2, \ldots, a_s, m \in \mathbb{Z} \setminus \{0\}$. *Entonces* $\mcd(\prod_{i=1}^{s} a_i, m) = 1$ *si y sólo si* $\mcd(a_i, m) = 1$ *para* $1 \leq i \leq s$.

□

Corolario 3.7. *Si* $\mcd(a,b) = 1$*, entonces* $\mcd(a^k, b^l) = 1$ *para todo* $k, l \in \mathbb{N}$.

□

Corolario 3.8. [Euclides] *Si* $\mcd(a,b) = 1$ *y* $a \mid bc$*, entonces* $a \mid c$.

□

Corolario 3.9. *Si* $a \mid c$, $b \mid c$ *y* $\mcd(a,b) = 1$*, entonces* $ab \mid c$.

□

Corolario 3.10. *Si* $c \neq 0$*, entonces* $\mcd(ca, cb) = |c| \mcd(a,b)$.

Demostración: Sea $d = \mcd(ca, cb)$, $d' = |c| \mcd(a,b)$ y $\mcd(a,b) = ax_0 + by_0$. Puesto que $ca = dt_0$ y $cb = dt_1$ se tiene $|c|a = \pm dt_0$ y $|c|b = \pm dt_1$, así que $d \mid |c|ax_0$ y $d \mid |c|by_0$. Por tanto $d \mid |c|(ax_0 + by_0)$, de donde $d \mid d'$. Falta ver que $d' \mid d$. Puesto que $|c| \mid c$ y $\mcd(a,b) \mid a$, se tiene que $|c| \mcd(a,b) \mid ca$. Análogamente $|c| \mcd(a,b) \mid cb$. Por el Teorema 3.3 se sigue que $|c| \mcd(a,b) \mid \mcd(ca, cb)$. Así que $d' \mid d$ y $d = d'$.

□

A continuación enunciamos algunas propiedades elementales del mcd.

Proposición 3.11. *Si* $a, b \in \mathbb{Z}$ *y al menos* a *ó* $b \neq 0$*, entonces*

1. $\mcd(a,b) = \mcd(b,a)$.
2. $\mcd(a,b) = \mcd(-a,b) = \mcd(|a|, |b|)$.

3. $\mathrm{mcd}(a,b) = |a|$ *si y sólo si* $a \mid b$.

4. $\mathrm{mcd}(a,0) = |a|$ *si* $a \neq 0$.

Demostración: Es un fácil ejercicio para el lector.

□

Teorema 3.12. *Sean* a, b *enteros ambos no cero. Si* $d \in \mathbb{Z}$ *es un divisor común de* a *y* b *tal que, siempre que* $c \mid a$ *y* $c \mid b$ *se tiene que* $c \mid d$*, entonces* $d = \pm \mathrm{mcd}(a,b)$.

Demostración: Si $g = \mathrm{mcd}(a,b)$ se tiene que $g \mid d$. Sea $g = ax_0 + by_0$. Entonces $d \mid ax_0 + by_0$. Así, por el Teorema 2.7 parte 5, $|g| = |d|$.

□

Aclaramos que las condiciones sobre d en el Teorema 3.12 junto con la condición $d > 0$ pueden ser tomadas como la definición de mcd. Sin embargo, esta definición también depende del orden en $\mathbb{Z}$ y de que cualquier entero diferente de 0 sólo tiene un número finito de divisores.

Comentario para aquellos lectores que entienden el lenguaje de los anillos: En un dominio entero arbitrario D, el Teorema 3.12 es la definición de mcd y ésta aparece en casi todos los textos clásicos de álgebra moderna.

El siguiente caso es un ejemplo de dominio entero en el cual dos elementos no tienen mcd. Vamos a suponer que la ecuación $x^2 - 10y^2 = \pm 3$ no tiene soluciones enteras x, y (ver ejercicio 2 en la penúltima lista de problemas del Capítulo 2). Sea $\mathcal{O}_{10} = \{m + n\sqrt{10} : m, n \in \mathbb{Z}\}$. Entonces $\mathcal{O}_{10}$ es un dominio entero con la suma y producto usual de números reales. Se tiene que:

1. Si $a + b\sqrt{10} \mid c + d\sqrt{10}$ en $\mathcal{O}_{10}$, entonces $a^2 - 10b^2 \mid c^2 - 10d^2$ en $\mathbb{Z}$.

2. 2 y $4 + \sqrt{10}$ son divisores en común de 6 y $8 + 2\sqrt{10}$ en $\mathcal{O}_{10}$. En efecto pues $6 = 2 \cdot 3$, $8 + 2\sqrt{10} = 2(4 + \sqrt{10})$, $6 = (4 + \sqrt{10})(4 - \sqrt{10})$.

3. Si $2 \mid a + b\sqrt{10}$ en $\mathcal{O}_{10}$, entonces $2 \mid a$ y $2 \mid b$ en $\mathbb{Z}$.

4. Si $4 + \sqrt{10} \mid 2c + 2d\sqrt{10}$ en $\mathcal{O}_{10}$, entonces $3 \mid c^2 - 10d^2$ en $\mathbb{Z}$. En efecto, aplicando el inciso 1 tenemos que $6 \mid 4(c^2 - 10d^2)$ en $\mathbb{Z}$, por tanto $3 \mid c^2 - 10d^2$ en $\mathbb{Z}$.

5. Si $2c + 2d\sqrt{10} \mid 6$ en $\mathcal{O}_{10}$, entonces $c^2 - 10d^2 \mid 9$ en $\mathbb{Z}$.

6. Si $2c + 2d\sqrt{10} \mid 8 + 2\sqrt{10}$ en $\mathcal{O}_{10}$, entonces $c^2 - 10d^2 \mid 6$ en $\mathbb{Z}$.

Usando lo anterior mostraremos que no existe un elemento en $\mathcal{O}_{10}$ el cual es divisor común de 6 y $8 + 2\sqrt{10}$ y que sea divisible por 2 y $4 + \sqrt{10}$ en $\mathcal{O}_{10}$. Supongamos que $a + b\sqrt{10} \mid 6$, $a + b\sqrt{10} \mid 8 + 2\sqrt{10}$ y $2 \mid a + b\sqrt{10}$, $4 + \sqrt{10} \mid$

$a + b\sqrt{10}$. Puesto que $2 \mid a + b\sqrt{10}$ en $\mathcal{O}_{10}$, entonces $2 \mid a$ y $2 \mid b$. Por tanto $a+b\sqrt{10} = 2c+2d\sqrt{10}$. Como $4+\sqrt{10} \mid 2c+2d\sqrt{10}$ en $\mathcal{O}_{10}$, entonces $3 \mid c^2-10d^2$ en $\mathbb{Z}$. Esto implica que $c^2 - 10d^2 \neq \pm 1$.

Por otro lado tenemos que $2c + 2d\sqrt{10} \mid 6$ en $\mathcal{O}_{10}$. Entonces $c^2 - 10d^2 \mid 9$ en $\mathbb{Z}$. También tenemos que $c^2 - 10d^2 \mid 6$ en $\mathbb{Z}$, entonces $c^2 - 10d^2 \mid 9 - 6$; es decir, $c^2 - 10d^2 \mid \pm 3$. Puesto que $3 \mid c^2 - 10d^2$ en $\mathbb{Z}$, entonces necesariamente $c^2 - 10d^2 = \pm 3$ y esta ecuación no es soluble en $\mathbb{Z}$.

En conclusión, 6 y $8 + 2\sqrt{10}$ no tienen mcd en $\mathcal{O}_{10}$. En $\mathbb{Z}$ ésto no puede suceder y la razón es porque $\mathbb{Z}$ es un dominio de factorización única: cualquier entero que no sea $0, 1, -1$ se puede expresar en forma única (salvo el orden y signo) como un producto finito de números primos.

Lema 3.13. *Sean $a, b \in \mathbb{Z}$ y escribimos $a = bq + r$ con $0 \leq r < |q|$. Entonces* $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Demostración: Sea $g = \text{mcd}(a, b)$ y $g_1 = \text{mcd}(b, r)$. Mostraremos que $g \mid g_1$ y $g_1 \mid g$. Puesto que $g \mid a$ y $g \mid b$, se tiene $g \mid a - bq$. Por tanto $g \mid b$ y $g \mid r$ y así $g \mid g_1$. Análogamente $g_1 \mid g$.

□

¿Fue necesaria la condición $0 \leq r < |q|$?

Teorema 3.14. [Algoritmo de Euclides] *Sean a, b enteros diferentes de 0. Entonces, después de aplicar el algoritmo de la división varias veces obtenemos*

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < |b|,\\
b &= r_1q_2 + r_2 && 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3 && 0 < r_3 < r_2,\\
&\vdots \quad \vdots &&\\
r_{k-2} &= r_{k-1}q_k + r_k && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_kq_{k+1}, &&
\end{aligned}$$

y $r_k = \text{mcd}(a, b)$.

Demostración: Tenemos una sucesión decreciente de enteros positivos

$$0 < r_k < r_{k-1} < \ldots < r_2 < r_1 < |b|,$$

y por razones obvias en algún momento obtenemos un residuo $r_{k+1} = 0$, es decir, este procedimiento termina en un número finito de pasos. De paso observemos que del último renglón tenemos $\text{mcd}(r_{k-1}, r_k) = r_k$ pues $r_k \mid r_{k-1}$. Aplicando el Lema 3.13 concluimos:

$$\text{mcd}(a, b) = \text{mcd}(b, r_1) = \text{mcd}(r_1, r_2) = \cdots = \text{mcd}(r_{k-1}, r_k) = r_k.$$

□

Un ejemplo con números pequeños será suficiente para ilustrar como se usa el Algoritmo de Euclides:

Ejemplo 3.15. *Calculemos* $\text{mcd}(-387, 578)$*:*

$$\begin{aligned} 578 &= -387(-1) + 191, \\ -387 &= 191(-3) + 186, \\ 191 &= 186(1) + 5, \\ 186 &= 5(37) + 1, \\ 5 &= 1(5). \end{aligned}$$

y por lo tanto, el último residuo diferente de 0 *es* $1 = \text{mcd}(-387, 578)$*.*

3.1 La ecuación $ax + by = c$

La geometría, una de las disciplinas más bellas de la matemática, nutre en muchas ocasiones, de problemas a la aritmética. ¿Cuántas veces se nos ha presentado la necesidad de encontrar las soluciones enteras de una ecuación del tipo $ax+by = c$ con $a, b, c \in \mathbb{Z}$ y que proviene de una situación real? Claramente este tipo de ecuaciones tienen una infinidad de soluciones en $\mathbb{Q}$, pero en $\mathbb{Z}$ no es tan evidente distinguirlas. Por ejemplo, imaginemos que cierto día de la semana, un banco sólo tiene billetes de 20 y 100 pesos y un cajero debe pagar un cheque de 2010 pesos. ¿Cuántos billetes de 20 y 100 debe dar? El cajero resolverá su problema si logra encontrar una solución de la ecuación $20x + 100y = 2010$. Si $x = 5$ y $y = \dfrac{191}{10}$, entonces ¿qué sentido tiene dar $\dfrac{191}{10}$ billetes de 100 pesos? ¿existe algún criterio que le asegure al cajero que podrá pagar el cheque?

Nuestro siguiente resultado nos brinda un criterio eficiente para decidir si la recta $ax+by = c$ pasa por puntos en el plano cartesiano con ambas coordenadas x, y enteros.

Teorema 3.16. *Sean* $a, b, c \in \mathbb{Z}$*. La recta* $ax + by = c$ *contiene puntos con coordenadas enteros si y sólo si* $\text{mcd}(a, b) \mid c$*.*

Demostración: Si x_0, y_0 son tales que $ax_0 + by_0 = c$, entonces es claro que $\text{mcd}(a, b) \mid c$. Inversamente, sea $g = \text{mcd}(a, b)$ y supongamos que $c = gt_0$. Usando el algoritmo de Euclides podemos encontrar $x_0, y_0 \in \mathbb{Z}$ tal que $ax_0 + by_0 = g$. Por lo tanto

$$c = gt_0 = a(x_0t_0) + b(y_0t_0)$$

y así, el punto de coordenadas (x_0t_0, y_0t_0) tiene coordenadas enteros y se encuentra sobre la recta $ax + by = c$.

□

Supongamos ahora que nuestra ecuación $ax + by = c$ es soluble en $\mathbb{Z} \times \mathbb{Z}$. Vamos a caracterizar todas las soluciones.

Corolario 3.17. *Sea x_0, y_0 una solución de $ax + by = c$ encontrada como en el teorema anterior. Sea $g = \text{mcd}(a, b)$ y $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ cualquier otra solución. Si $a = ga_1$ y $b = gb_1$, entonces $x = x_0 - b_1t$, $y = y_0 + a_1t$, para algún $t \in \mathbb{Z}$.*

Demostración: De la igualdad $ax_0 + by_0 = ax + by$ se sigue que

$$a(x_0 - x) = b(y - y_0).$$

Por lo tanto $a_1(x_0 - x) = b_1(y - y_0)$. Puesto que $\text{mcd}(a_1, b_1) = 1$ obtenemos

$$b_1 \mid x_0 - x \quad \text{y} \quad a_1 \mid y - y_0.$$

Por lo anterior $x_0 - x = b_1t$. Así $a_1b_1t = b_1(y - y_0)$ y cancelando llegamos a que $a_1t = y - y_0$.

□

Observemos que si tenemos una solución particular x_0, y_0 de la ecuación $ax + by = c$, entonces para cualquier $t \in \mathbb{Z}$ se tiene que $x_0 - b_1t$ y $y_0 + a_1t$ proporciona todas las soluciones de nuestra ecuación.

El Teorema 3.16 se puede expresar en forma más general.

Teorema 3.18. *Sean $a_1, a_2, \ldots a_n, c \in \mathbb{Z}$. La ecuación $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ es soluble en $\mathbb{Z} \times \ldots \times \mathbb{Z}$ si y sólo si $\text{mcd}(a_1, a_2, \ldots, a_n) \mid c$.*

Demostración: Es idéntica a la del Teorema 3.16.

□

4 Mínimo común múltiplo

Sean $a_1, ..., a_k$ enteros diferentes de 0. Cualquier entero x tal que $a_i \mid x$, $(i = 1, ..., k)$ es llamado *múltiplo común* de los a_i's. Consideremos el conjunto $S = \{x \in \mathbb{N} : a_i \mid x\}$. Entonces el entero

$$|\prod_{i=1}^{k} a_i| \in S,$$

y así $S \neq \emptyset$. Por el **PBO** existe $N \in S$ tal que $N \leq x$ para todo $x \in S$.

Definición 4.1. *El entero N de la discusión anterior se llama el mínimo común múltiplo (*mcm*) de los enteros $a_1, ..., a_k$ y lo denotamos como* $\text{mcm}(a_1, ..., a_k)$.

¿Por que pedir que los a_i's sean diferentes de 0?

El mcm tiene la siguiente propiedad que lo caracteriza:

Teorema 4.2. *Sean $a_1, ..., a_k$ enteros diferentes de 0 y $N = \text{mcm}(a_1, ..., a_k)$. Si c es cualquier múltiplo común de los a_i's, entonces $N \mid c$.*

Demostración: Supongamos que existe un múltiplo común M de los a_i's tal que $N \nmid M$. Por el algoritmo de la división tenemos $M = Nq + r$ con $0 < r < N$. Como M, N son múltiplos comunes de los a_i's, entonces existen enteros x_i, y_i tal que $M = x_i a_i, N = y_i a_i$ con $i = 1, ..., k$. De lo anterior se sigue que r es un múltiplo común positivo de los a_i's y $r < N$ lo cual es absurdo.

□

Teorema 4.3. *Sean a_1, a_2 enteros no nulos. Entonces el número* $\dfrac{|a_1 a_2|}{\text{mcd}(a_1, a_2)}$ *tiene las siguientes propiedades :*

1. $\dfrac{|a_1 a_2|}{\text{mcd}(a_1, a_2)}$ *es un entero positivo.*
2. $a_i \mid \dfrac{|a_1 a_2|}{\text{mcd}(a_1, a_2)}$, $i = 1, 2$.
3. *Si $x \in \mathbb{Z}$ satisface que $a_1 \mid x$ y $a_2 \mid x$, entonces* $\dfrac{|a_1 a_2|}{\text{mcd}(a_1, a_2)} \mid x$.

Demostración: Para la primera parte observemos que $\text{mcd}(a_1, a_2) \mid |a_1|$. Por lo tanto $\text{mcd}(a_1, a_2) \mid |a_1 a_2|$. La segunda afirmación se sigue directamente de:

$$\frac{|a_1 a_2|}{\text{mcd}(a_1, a_2)} = \pm a_1 \frac{|a_2|}{\text{mcd}(a_1, a_2)} = \pm a_2 \frac{|a_1|}{\text{mcd}(a_1, a_2)}.$$

Para la tercera afirmación consideremos $d = \text{mcd}(a_1, a_2)$ con

$$a_1 = dq_1, \quad a_2 = dq_2, \quad x = a_1 r = a_2 t, \quad \text{mcd}(q_1, q_2) = 1.$$

Puesto que $a_1 r = dq_1 r = a_2 t = dq_2 t$, entonces $q_1 \mid q_2 t$. Por lo tanto $q_1 \mid t$ y $t = q_1 s$. De la igualdad

$$x = a_2 t = dq_2 t = s(dq_1 q_2) = s\frac{a_1 a_2}{d},$$

se sigue el resultado.

□

Corolario 4.4. *Si* $N = \text{mcm}(a_1, a_2)$*, entonces* $N = \dfrac{|a_1 a_2|}{\text{mcd}(a_1, a_2)}$.

□

Del Corolario 4.4 obtenemos la fórmula $\text{mcm}(a_1, a_2)\,\text{mcd}(a_2, a_1) = |a_1 a_2|$. Sin embargo observemos:

$$48 = \text{mcm}(4, 4, -12)\,\text{mcd}(4, 4, -12) \neq 192 = |4 \cdot 4 \cdot (-12)|,$$

así que el Corolario 4.4 no es válido para más de dos enteros.

Corolario 4.5. *Si* $a, b, m \neq 0$*, entonces*

$$\text{mcm}(ma, mb) = |m|\text{mcm}(a, b).$$

Demostración: Usar 3.10

□

¿Hace falta un algoritmo para calcular el mcm de dos enteros?

5 Teorema Fundamental de la Aritmética

Cualquier entero $a \neq 0, \pm 1$ tiene al menos cuatro divisores: $\pm 1, \pm a$. Si un entero a tiene al menos un divisor $b \neq \pm a, \pm 1$, entonces $a = bd$ y $d \neq \pm a \pm 1$.

Definición 5.1. *Sea* $a \neq 0, \pm 1$*. Diremos que* a *es un número primo si* $a = bd$*, entonces* $b = \pm 1$ *ó* $d = \pm 1$*. En caso contrario diremos que* a *es compuesto.*

Tenemos que los primeros números primos positivos son: $2, 3, 5, 7, 11, ...$, pero también $-2, -3, -5, -11, ...$ son números primos. Así que es claro que n es primo si y sólo si $-n$ es primo. Por esta razón, será suficiente estudiar los números primos positivos. Reservamos el uso de las letras p y q para indicar números primos. Refraseando la definición de número compuesto: si $n \neq \pm 1$ es compuesto, entonces n admite un divisor b diferente de ± 1 y $\pm n$.

Teorema 5.2. *Cualquier entero* $m > 1$ *admite al menos un divisor primo.*

Demostración: Inducción sobre m. Si $m = 2$, no hay nada que probar. Supongamos que $m > 2$ admite al menos un divisor primo p. Si $m+1$ es primo, terminamos. Si $m+1$ es compuesto, existe a tal que $1 < a < m+1$ y $a \mid m+1$. Pero $a \leq m$. Así que a admite al menos un divisor primo p y por lo tanto $p \mid m+1$.

□

Teorema 5.3. [Euclides] *p es primo si y sólo si siempre que $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.*

Demostración: Supongamos que p es primo y $p \mid ab$. Si $p \nmid a$, entonces $\text{mcd}(a, p) = 1$ y por el Corolario 3.8 tenemos que $p \mid b$.

Inversamente, sea $p = ab$ una factorización de p. En particular $p \mid ab$ y por lo tanto $p \mid a$ ó $p \mid b$. Si $p \mid a$ se tiene que $a = pt$, para algún $t \in \mathbb{N}$. Así que $p = ab = ptb$. De lo anterior se sigue que $b = 1$ y $a = p$ y por lo tanto p es primo.

□

La propiedad más importante de $\mathbb{Z}$ se refiere a la factorización única de sus elementos.

Corolario 5.4. [Teorema Fundamental de la Aritmética] *Todo entero positivo se puede expresar en forma única (salvo el orden) como un producto finito de números primos.*

Demostración: Sólo hay que probar la unicidad. Supongamos que

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_s.$$

Si en la factorización de n suponemos que $k < s$, entonces sabiendo que $p_1 \mid q_1 q_2 \cdots q_s$ obtenemos $p_1 = q_j$ para algún $1 \leq j \leq s$. Reordenando los subíndices si es necesario, podemos suponer que $p_1 = q_1$. Después de cancelar y repitiendo este proceso obtenemos

$$p_1 = q_1, \quad p_2 = q_2, \ \ldots, p_k = q_k.$$

De esta manera llegamos a $1 = q_{k+1} q_{k+2} ... q_s$, lo cual es imposible. Similarmente $k > s$ nos conduce a un absurdo y así se obtiene el resultado.

□

Corolario 5.5. *Si $n > 2$, entonces existe un primo p tal que $n < p < n!$.*

Demostración: El número $z = n! - 1 > 1$ tiene un divisor primo $p \leq z$. Si $p \leq n$, entonces $p \mid n!$ y por lo tanto $p \mid 1$ lo cual es absurdo. Así que $n < p \leq n! - 1 < n!$.

□

Corolario 5.6. [Teorema de Euclides] *Existe una infinidad de números primos.*

Demostración: Consideremos n suficientemente grande en el corolario anterior.

□

La proposición 20 del libro IX de los *Elementos* de Euclides [10] afirma lo mismo que el Corolario 5.6. La demostración que da Euclides es la siguiente: Supongamos que $p_1, p_2, ..., p_r$ son todos los números primos y considera el entero $N = 1+p_1 \cdot p_2 \cdots p_r$. El Teorema 5.2 garantiza que N admite al menos un divisor primo el cual debe ser alguno de $p_1, p_2, ..., p_r$ y ninguno de éstos divide a N. Así que debe existir al menos otro primo diferente de los conocidos $p_1, p_2, ..., p_r$. La prueba que dió Kummer en 1878 [19] acerca de la infinitud de los números primos es igual de bella que la de Euclides: Supongamos que existe un número finito de primos $p_1, p_2, \ldots, p_r$ y sea $N = p_1 p_2 \cdots p_r$. El entero $N - 1$ tiene un factor primo en común p_i con N. Así que p_i divide a $N - (N - 1) = 1$, lo cual no es posible. Obviamente la prueba de Kummer es una ligera variación de la de Euclides. En el problema 83 describiremos otra variación de la prueba de Euclides la cual resulta más interesante.

¿Cómo averiguar si un número entero positivo es compuesto o primo? La respuesta final no ha sido encontrada. Gracias a esto, el estudio de la teoría de los números primos, actualmente es una de las áreas de la matemática que ha encontrado aplicaciones en otras disciplinas, como la *criptografía*. Esta rama de la matemática aplicada estudia los métodos para cifrar mensajes secretos por medio de una clave secreta, de tal forma que sólo puedan ser descifrados por un receptor. Al receptor sólo le hace falta aplicar la clave secreta al revés. En 1977 Ronald Rivest, Adi Shamir y Leonard Adleman [35], matemáticos del Massachusetts Institute of Technology, descubrieron que los números primos eran idóneos para el proceso de cifrar fácil y descifrar difícil. En la actualidad nadie puede cuestionar la importancia de distinguir a un número primo de un número compuesto. Una parte de las investigaciones actuales en aritmética, consiste en encontrar algoritmos eficientes para factorizar números enteros grandes para ser utilizados en ataques a sistemas criptográficos, que son, por ejemplo, el corazón de los sistemas de pago de las tarjetas de crédito.

En biología también han aparecido los números primos, por ejemplo, para interpretar el ciclo de vida de las cigarras. La especie *septendecim* tiene un ciclo de vida de 17 años. Este ciclo comienza bajo tierra en donde la ninfa de la cigarra se alimenta succionando las raíces de los árboles. Después de 17 años, sale a la superficie para aparearse, poner sus huevecillos y finalmente morir. Esto sólo le lleva unas cuantas semanas. La especie *tredecim* tiene un ciclo de vida de 13 años y después de este tiempo, se comporta de la misma manera que sus hermanas *septendecim*. Es obvio que el nombre asignado a cada una de éstas tiene que ver con la duración de su ciclo de vida. ¿Por qué la cigarra tiene un ciclo de vida tan largo? ¿Qué interpretación tiene el hecho que su ciclo de vida dure un número primo de años?

Una teoría sugiere que la cigarra tiene un parásito que también tiene un ciclo de vida y la cigarra está tratando de evitarlo. La parte importante de este hecho asombroso es que el tiempo reproductivo de la cigarra es justamente unas semanas después de 17 años (en el caso de *septendecim*). Es en este momento cuando el supuesto parásito puede hacer de las suyas. Por ejemplo, si el parásito tiene un ciclo de vida de 4 años, entonces la cigarra busca evitar un ciclo de vida que sea divisible por 4. Aún así la cigarra y el parásito coincidirán después de $4 \times 17 = 68$ años.

Se cree también que el parásito se defiende y que tiene un ciclo de vida que debe incrementar la frecuencia de coincidencia. Al respecto existen muchas especulaciones e invitamos al lector a seguir esta interesante teoría [23].

En la actualidad se conocen algunos métodos para verificar si un entero dado n es primo o no. Por ejemplo, el Teorema 5.3 puede ser considerado como una prueba de primacidad que es muy difícil de implementar en la práctica.

El siguiente método es elemental y también puede ser considerado como una prueba de primacidad. Desafortunadamente su implementación en enteros grandes lo hace poco eficiente.

Teorema 5.7. *Si n es compuesto, entonces n admite al menos un divisor primo p tal que $p \leq \sqrt{n}$.*

Demostración: Supongamos que $n = p_1 p_2 \cdots p_s$ y que $p_1 \leq p_2 \leq ... \leq p_s$, entonces claramente $p_1^2 \leq n$ y así $p_1 \leq \sqrt{n}$.

□

Del Teorema 5.7 se deduce fácilmente que si para un entero positivo n no existe un primo p con $p \leq \sqrt{n}$ y tal que $p \mid n$, entonces necesariamente n debe ser primo.

Un método elemental para encontar números primos consecutivos fué dado por Eratóstenes[2]. Consideremos la sucesión $2, 3, 4, ...$ Denotamos por $p_1 = 2$, el cual es el primer número primo. Quitemos de la sucesión a todos lo números mayores que p_1 y que son múltiplos de 2. El primero de los números restantes es $p_2 = 3$. Nuevamente quitemos de la sucesión a todos los números mayores que p_2 y que son múltiplos de p_2. El primero de los números restantes es $p_3 = 5$. Supongamos que después del k-ésimo paso encontramos el k-ésimo primo p_k. Quitemos de la sucesión a todos los números mayores que p_k y que son divisibles

[2]Eratóstenes nace en el año 276 a.c en Cirene, hoy Libia. Estudia en Alejandría y Atenas y después se hace director de la Biblioteca de Alejandría. Escribe poesía, es historiador, geógrafo, matemático, astrónomo y atleta. Trabajó en problemas como la duplicación del cubo y los números primos. Escribió muchos trabajos de los cuales sólo se tiene referencia por medio de citas de otros autores. Su poema más famoso es *Hermes* el cual está inspirado en observaciones astronómicas. En su vejez queda ciego y muere de hambre por su propia voluntad en el año 194 a.c.

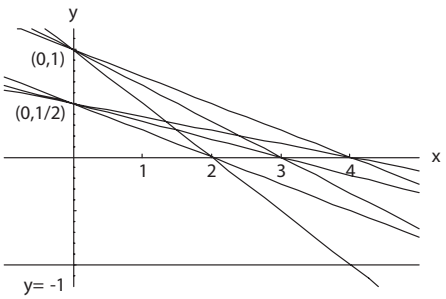
por p_k. En particular, $p_{319} = 4397$ [33]. El método descrito anteriormente es conocido como la *criba de Eratóstenes*.

Según el diccionario de la Real Academia de la Lengua Española, edición del año 2001, una criba es "un cuero ordenadamente agujereado y fijo a un aro de madera que sirve para limpiar el trigo u otras semillas ". Así, la criba de Eratóstenes es un método que sirve para limpiar de números compuestos a los enteros positivos. Por supuesto que no queremos despreciar a los números compuestos, simplemente nos es suficiente conocer a los números primos pues ellos son, en cierto sentido, un conjunto de generadores de los números enteros.

En seguida daremos la construcción de una criba geométrica que funciona de la misma manera que la de Eratóstenes. Consideremos en el plano cartesiano los conjuntos

$$A = \left\{ (0, \frac{1}{m}) : m = 1, 2, ... \right\}, \quad B = \{(n+1, 0) : n = 1, 2, ...\},$$

donde cada punto del conjunto A está conectado por una recta con cada punto del conjunto B (ver figura).



La ecuación de la recta que pasa por los puntos $(n+1, 0)$ y $(0, \frac{1}{m})$ está descrita por

$$y = -\frac{1}{m(n+1)}x + \frac{1}{m},$$

y la intersección de $y = -\frac{1}{m(n+1)}x + \frac{1}{m}$ con la recta $y = -1$ es el punto con coordenadas $((m+1)(n+1), -1)$.

Observemos que las abscisas de estos puntos son precisamente números compuestos. Recíprocamente, si x es un entero positivo compuesto, entonces $x = (m+1)(n+1)$ satisface las ecuaciones

$$y = -\frac{1}{m(n+1)}x + \frac{1}{m},$$
$$y = -1.$$

Resumiendo: si z es entero positivo, L_1 denota la recta $y = -\frac{1}{m(n+1)}x + \frac{1}{m}$, y L_2 es la recta $y = -1$, entonces $(z, -1) \in L_1 \cap L_2$ si y sólo si z es compuesto.

6 Distribución de los números primos

Entre las razones que guían el interés por el estudio de los números primos hay dos que sobresalen: la primera, por ser un tema de la matemática básica moderna que ha despertado el interés de destacados especialistas y amateurs en el tema y la segunda, por sus aplicaciones.

Es relativamente fácil escribir listas de números primos. De hecho, existen programas computacionales y páginas en la red que nos proporcionan listas suficientemente grandes. Ve por ejemplo la estupenda página de la Universidad de Tennessee www.utm.edu/research/primes/. Una primera pregunta que nos haremos proviene de observar listas de primos. Consideremos los primos menores que 1000:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,
101, 103, 107, 109, 113, 127, 131, 137, 139, 149,
151, 157, 163, 167, 173, 179, 181, 191, 193, 197,
199, 211, 223, 227, 229, 233, 239, 241, 251, 257,
263, 269, 271, 277, 281, 283, 293, 307, 311, 313,
317, 331, 337, 347, 349, 353, 359, 367, 373, 379,
383, 389, 397, 401, 409, 419, 421, 431, 433, 439,
443, 449, 457, 461, 463, 467, 479, 487, 491, 499.
503, 509, 521, 523, 541, 547, 557, 563, 569, 571,
577, 587, 593, 599, 601, 607, 613, 617, 619, 631,
641, 643, 647, 653, 659, 661, 673, 677, 683, 691,
701, 709, 719, 727, 733, 739, 743, 751, 757, 761,

769, 773, 787, 797, 809, 811, 821, 823, 827, 829,
839, 853, 857, 859, 863, 877, 881, 883, 887, 907,
911, 919, 929, 937, 941, 947, 953, 967, 971, 977,
983, 991, 997.

Observamos que entre 1 y 100 hay 25 primos, entre 100 y 200 hay 21, entre 200 y 300 hay 16, entre 300 y 400 hay 16, entre 400 y 500 hay 17 primos, entre 500 y 600 hay 14, entre 600 y 700 hay 16, entre 700 y 800 hay 14, entre 800 y 900 hay 15 y finalmente entre 900 y 1000 hay 14. Pareciera a primera vista, que cada bloque de 100 enteros contiene *casi* la misma cantidad de primos. Sin embargo observemos el siguiente hecho:

$$k! + n \quad \text{es un número compuesto para} \quad n = 2, \ldots, k.$$

Por lo tanto, la lista de primos que presentamos, es engañosa. Existen grandes bloques de enteros consecutivos en donde no hay uno sólo de ellos. Esto significa que para n muy grande ¿n es compuesto? Si sabemos que hay una infinidad de ellos, entonces ¿cómo están distribuidos dentro de $\mathbb{Z}$? Afortunadamente este misterio ha convertido a la teoría de números en una de las ramas fundamentales de la matemática actual.

Tal vez una de las razones de la irregularidad de la distribución de los números primos es que no existe una fórmula simple que los reproduzca (ver por ejemplo el problema 98 al final de este capítulo). Debemos mencionar que han habido intentos por reproducirlos en su totalidad por medio de expresiones polinomiales en varias variables [18]. En los siglos XVIII y XIX, el estudio de la distribución de los primos fue objeto de muchas especulaciones; prácticamente todas las investigaciones estaban encaminadas a encontrar una fórmula que reprodujera primos. Para estudiar esta distribución sea $x \in (1, \infty)$ y consideremos la función

$$\pi(x) = \sum_{\substack{p \leq x \\ p \text{ primo}}} 1.$$

Esta *inofensiva* función lo único que hace es contar los primos $p \leq x$. Puesto que existe una infinidad de ellos, es claro que si x crece, entonces la función $\pi(x)$ también crece más que cualquier cota superior asignada. Fue precisamente Gauss y Legendre los que, en base a tablas, proponen una nueva pregunta: ¿existirá una fórmula que cuente números primos? Ellos conjeturaron que la función $\pi(x)$ y $\dfrac{x}{\log(x)}$ se parecen mucho cuando x es muy grande, donde $\log x$ es la función ln. Cada uno de ellos propuso fórmulas diferentes y la mejor estimación fue la fórmula propuesta por Gauss. Este hecho lo podemos escribir como

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

Probar que este límite existe y es igual a 1 es algo muy difícil y queda fuera del alcance de este trabajo.

En 1859 Riemann[3] comienza en forma sistemática el estudio de éste problema y lo asocia con la función

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

donde $s \in \mathbb{C}$ y la parte real de $s > 1$ para que la serie sea convergente.

Riemann, en su intento por dar respuesta al comportamiento de la distribución de los números primos, logra desarrollar con bastante éxito la teoría general de funciones de una variable compleja. Su teoría, aún en la actualidad, contiene argumentos obscuros. Un estupendo punto de vista acerca del trabajo de Riemann se puede consultar en [46].

El trabajo de Riemann es completado al final del siglo XIX. Hadamard[4] se interesa en el problema de la distribución de los números primos y en el camino desarrolla la teoría de las funciones enteras y demuestra, casi simultáneamente con Vallée Poussin, que

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

Este famoso resultado es conocido como *El Teorema de los Números Primos*. Después de la demostración de *El Teorema de los Números Primos*, hecha por Hadamard y Vallée Poussin, los matemáticos buscaron clarificar la conección entre la teoría de funciones de una variable compleja y la distribución de los

[3]George Friedrich Bernhard Riemann nació el 17 de septiembre de 1826 en Breselenz (Hannover), Alemania. Su padre, ministro de la iglesia Luterana, se encargó de la educación de sus hijos hasta los diez años. El 1846 Riemman ingresa a la Universidad de Göttingen en donde, en 1849, Gauss le dirije su tesis doctoral sobre la teoría de variable compleja. En 1847 hace estudios en la Universidad de Berlín teniendo como profesores a Steiner, Jacobi, Dirichlet y Eisenstein. Ingresa como profesor en Göttingen reemplazando a Dirichlet. Muere de tuberculosis en el año 1866 en Selasca, Italia.

[4]Jackes Hadamard nació el año 1895 en Versalles, Francia. Su trabajo ocupa un lugar destacado en la matemática. Sus principales aportaciones fueron en ecuaciones diferenciales parciales pero también se le recuerda porque fue el primero (junto con Vallée Poussin) en haber demostrado el Teorema de los Números Primos. Su vida privada estuvo llena de tragedias y a pesar de esto su trabajo logra el aprecio de los matemáticos más importantes de su época. Muere en Paris el 15 de octubre de 1963. Sugerimos al lector buscar una biografía de Hadamard.

números primos. La demostración depende esencialmente del estudio de los ceros de la función zeta de Riemann[46]. A finales del siglo XIX, se creía que la teoría de las funciones analíticas era más profunda que el análisis real. Por esta razón, en aquella época se pensaba que era imposible dar una demostración de *El Teorema de los Números Primos* sólo con manipulaciones de igualdades y desigualdades.

En 1949 A. Selberg y P. Erdös [36] [9], por separado, dan una demostración "elemental", que de ninguna manera era fácil, poniendo en entredicho la importancia de la teoría de las funciones analíticas. En la actualidad, en libros de variable compleja o de análisis es posible encontrar una demostración de este importante teorema. Recomendamos al lector revisar el estupendo libro de G. Tenenbaum y M.M. France [42].

Regresando al siglo XIX, en el año 1851 Chebyshev, en su intento por demostrar la conjetura de Gauss y Legendre sobre la distribución de los números primos, muestra que existen constantes positivas c y C tales que

$$c\frac{x}{\log(x)} < \pi(x) < C\frac{x}{\log(x)},$$

para $x \geq 2$. También muestra que si el límite existe, cuando $x \to \infty$, entonces $c = C = 1$. Se puede verificar que con los valores $c = 0.921$ y $C = 1.106$ la desigualdad anterior proporciona una evidencia numérica importante.

En este orden de ideas, en 1845 Joseph Bertrand conjeturó que existe al menos un primo entre n y $2n$. Él verificó su afirmación para $n < 3000000$. Esta conjetura fue demostrada por Chebyshev en 1850.

Esta breve historia nos servirá como marco de referencia para enfrentar dos hechos que podrían tambalear nuestra intuición: el Postulado de Bertrand contra la existencia de grandes espacios de enteros consecutivos que no contienen números primos. Hemos decidido posponer este enfrentamiento hasta el final del capítulo 2 porque es necesario el uso de la función φ de Euler.

PROBLEMAS

1. Mostrar que la siguiente versión del Principio de Inducción es equivalente a la que dimos al principio del capítulo: Sea $P(n)$ una proposición acerca del entero positivo n. Supongamos que $P(1)$ es verdadera. Si $P(n)$ es verdadera implica que $P(n+1)$ es verdadera, entonces la proposición P es verdadera para todos los enteros positivos.

2. Demostrar las siguientes fórmulas usando inducción matemática:

a) Sea $n \geq 1$ y $S_1(n) = \sum_{i=1}^{n} i$. Entonces $S_1(n) = \dfrac{n(n+1)}{2}$.

b) Sea $n \geq 1$ y $S_2(n) = \sum_{i=1}^{n} i^2$. Entonces $S_2(n) = S_1(n)\dfrac{2n+1}{3}$.

c) Sea $n \geq 1$ y $S_3(n) = \sum_{i=1}^{n} i^3$. Entonces $S_3(n) = (S_1(n))^2$.

d) Si $S_4(n) = \sum_{i=1}^{n} i^4$, entonces $S_4(n) = S_1(n)\dfrac{6n^3+9n^2+n-1}{15}$.

3. Demostrar que para $n \geq 1$ se cumple

$$(n+1)^{k+1} - n^{k+1} = (k+1)n^k + \binom{k+1}{2}n^{k-1} + \cdots + \binom{k+1}{k}n + 1.$$

4. Sea $n \geq 1$ y supongamos que $S_1(n), ..., S_{k-1}(n)$ son conocidos. Demostrar que:

a) $$(n+1)^{k+1} - 1 = \binom{k+1}{1}S_k(n) + \binom{k+1}{2}S_{k-1}(n) + \cdots + \binom{k+1}{k-1}S_2(n) + \binom{k+1}{k}S_1(n) + n.$$

Sugerencia: evaluar en el Problema 3 desde 1 hasta n y luego sumar.

b) Usar el inciso anterior para deducir una fórmula para $S_5(n)$ y en general, para $S_k(n)$. Debemos anunciarle al lector que las sumas $S_k(n)$ tienen que ver con la función ζ de Riemann, los primos regulares y con la demostración del llamado *primer caso del Teorema de Fermat.* Hacemos la invitación a leer el Capítulo 15 de [17]

5. Usar inducción para demostrar que:

a) Para cualquier entero $n \geq 3$ se cumple que $n^2 > 2n + 1$.

b) Para cualquier entero $n \geq 5$ se cumple que $2^n > n^2$.

c) $1 + 3 + \cdots + (2n-1) = n^2$.

d) $2 + 4 + 6 + \cdots + 2n = n(n+1)$.

e) $1(1)! + 2(2)! + 3(3)! + \ldots + n(n)! = (n+1)! - 1$, para $n \geq 1$.

f) Si $r \neq 1$, $a + ar + ar^2 + \ldots + ar^n = \dfrac{a(r^{n+1}-1)}{r-1}$, para $n \geq 1$.

6. En 1883, el matemático francés Edouard Lucas, se hizo famoso con la invención de una bella leyenda conocida como *Las Torres de Hanoi*. Con el tiempo, la computación hizo uso del juego para estudiar la eficiencia de algunos algoritmos computacionales. Cuenta la leyenda que el dios

Brahma entregó a los monjes del gran templo de Varanasi[5] tres vástagos (varillas) de diamante encajados en una base de bronce. Ensartó en uno de los vástagos 64 discos de oro, todos de dimensiones diferentes, acomodados de tal forma que el mayor quedó en la base y los restantes, acomodados en forma decreciente en tamaño. Ordenó a los monjes que moviesen todos los discos a otro vástago, de tal forma que en cada movimiento sólo fuese movido un disco y no estuviera sobre éste, uno mayor. Brahma sentenció: *Cuando hayan terminado la tarea, el mundo se vendrá abajo como una montaña de polvo.*

a) ¿Cuál cree el lector que es la forma más eficiente de ir cambiando los discos de una varilla a otra?

b) Supongamos que en cada movimiento se utiliza un segundo. Demostrar que los monjes podrán pasar los 64 discos de un varilla a otra en $2^{64} - 1$ segundos ¿Cuánto es en años?

c) Supongamos que en una varilla hay n discos acomodados según la leyenda y que se utiliza 1 segundo en cada movimiento. Demostrar que los monjes podrán cambiarlos todos en $2^n - 1$ segundos.

7. Consideremos el siguiente triángulo:

$$\begin{array}{ccccc} 1 & & & & \\ 3 & 5 & & & \\ 7 & 9 & 11 & & \\ 13 & 15 & 17 & 19 & \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

Demostrar que la suma de las entradas del k-ésimo renglón es un cubo.

8. Considere la matriz $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Demostrar que $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

9. Sea $n \in \mathbb{N}$ y $f(n) = \dfrac{10^n - 1}{9}$. Demostrar que:

a) $f(n) = 11...1$. ¿Cuántos $1'$s aparecen?

b) Si $n \mid m$, entonces $f(n) \mid f(m)$.

c) Si n es compuesto, entonces $f(n)$ es compuesto.

d) Encontrar un ejemplo con n primo y $f(n)$ compuesto.

10. Usar el **PBO** para demostrar que 3 es el menor elemento del conjunto $S = \{6x + (-9)y > 0\}$.

11. Usar el algoritmo de la división para demostrar que:

[5] Ciudad santa de hinduismo situada entre los ríos Varana y Asi, conocida también como Benarés.

a) Cualquier entero de la forma $6n+5$ es de la forma $3n+2$ ¿Es cierto el inverso de esta afirmación?

b) El cuadrado de cualquier entero es de la forma $3k$ o bien $3k+1$ pero no de la forma $3k+2$.

c) Cualquier entero impar es de la forma $4n+1$ o bien $4n+3$.

d) El cuadrado de cualquier entero impar es de la forma $8n+1$.

12. Demostrar la Proposición 3.11.

13. Encontrar el mcd de los siguientes números y expresarlos como combinación lineal de ellos:

a) 17 y -43.

b) 130 y 45.

c) -39 y 0.

d) -25 y -32.

e) 15, -27 y 18.

14. Mostrar que $2^n \mid k$ si y sólo si 2^n divide al entero formado por los n primeros dígitos de k (de derecha a izquierda). Sugerencia: si $k = a_r a_{r-1} \dots a_0$, entonces $k = a_0 + a_1 10 + \cdots + a_r 10^r$.

15. Consideremos k como en el problema anterior. Demuestre que k deja residuo $0, 1, 2$ o 3 al ser dividido entre 4 si y sólo si el número formado por los 2 primeros dígitos de k deja residuo $0, 1, 2$ o 3 respectivamente al ser dividido entre 4.

16. Mostrar que $5^n \mid k$ si y sólo si 5^n divide al entero formado por los n primeros dígitos de k.

17. Mostrar que $9 \mid 10^n - 1$ para toda $n \geq 1$.

18. Mostrar que $3 \mid n$ si y sólo si 3 divide a la suma de los dígitos de n.

19. Mostrar que $9 \mid n$ si y sólo si 9 divide a la suma de los dígitos de n.

20. Mostrar que $6 \mid n$ si y sólo si $2 \mid n$ y $3 \mid n$.

21. Divisibilidad por 7. Sea $n = a_0 + a_1 10 + ... + a_r 10^r$ la representación decimal de n. Escribir $n = 10^2 a + b$, donde $b = a_0 + a_1 10$ es el número formado por los dos primeros dígitos de n. Mostrar que $7 \mid n$ si y sólo si $7 \mid 5a - b$.

22. Sea $n = \sum_{i=0}^{r} a_i 10^i$. Mostrar que $11 \mid n$ si y sólo si $11 \mid \sum_{i=0}^{r} (-1)^i a_i$.

23. Mostrar que $12 \mid n$ si y sólo si $3 \mid n$ y $4 \mid n$. ¿Se Puede generalizar?

24. Considerar n como en el Problema 20. Mostrar que $13 \mid n$ si y sólo si $13 \mid 4a - b$. Mostrar que $17 \mid n$ si y sólo si $17 \mid 2a - b$.

25. Usar los Problemas 20 y 23 para dar un criterio de divisibilidad por 19 y 23.

26. Considerar la sucesión $1, -3, -4, -1, 3, 4, 1, -3, -4, \ldots$ y $n = \sum_{i=0}^{r} a_i 10^i$. Demostrar que $13 \mid n$ si y sólo si $13 \mid a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + a_6 - 3a_7 - 4a_8 - \ldots$.

27. Sea $n \in \mathbb{Z}$.

    a) Mostrar que $2 \mid n(n+1)$.

    b) Mostrar que si $\text{mcd}(4, y) = 1$ y $x \mid 16$, $x \mid 4y^2$, entonces $x \mid 4$.

    c) Mostrar que 3 divide a alguno de los enteros n, $n+7$ ó $n+8$.

    d) Mostrar que n divide al producto de n enteros consecutivos.

28. Usar inducción para mostrar que:

    a) $7 \mid 2^{3n} - 1$.

    b) $3 \mid 2^n + (-1)^{n+1}$.

29. Encontrar todas las soluciones enteras de las siguientes ecuaciones:

    a) $3x + 7y = -2$.

    b) $-2x - 5y = 7$.

    c) $2x + 5y - 11z = 1$.

    d) $x - 14y - 7z = 4$.

30. Sean $a, b, c, d \in \mathbb{Z}$ y supongamos que la ecuación $ax + by + cz = d$ tiene al menos una solución en los enteros x_0, y_0, z_0. Caracterizar todas las soluciones.

31. Una persona tiene 77 pesos en monedas de 2 y 5 pesos. ¿Cuál es el número máximo y mínimo de monedas que puede tener? ¿es posible que el número de monedas de 2 pesos coincida con el número de monedas de 5 pesos?

32. Un cierto número de seises y nueves se suman para obtener el número 126. Si el número de seises y nueves que son sumados se intercambia, entonces se obtiene como suma al número 114. ¿Cuántos seises y nueves había en un principio?

33. Dos escalas están hechas con unidades de 4 y 9 cm. Si se hace coincidir el 0 ¿a cuántos cm. coincidirán exactamente las dos marcas? Si las escalas están hechas con unidades de n y m cm y si se hace coincidir el 0 cuál es la respuesta a la misma pregunta.

34. Demostrar que si $n \geq 5$, entonces $n!$ termina en 0. ¿En cuántos ceros termina 351!?

35. Mostrar que si n es impar, entonces $a+b \mid a^n+b^n$. ¿Qué se puede decir si n es par?

36. Si n es impar, entonces $5 \mid 2^{2n}+1$.

37. Mostrar que $x-y \mid x^n-y^n$.

38. Mostrar que la ecuación $x^n+y^n=z^{n-1}$ tiene una infinidad de soluciones enteras. Sugerencia: $[(a^n+b^n)^{n-1}]^{n-1}=(a^n+b^n)^{n^2-2n+1}$.

39. Mostrar que la ecuación $x^n+y^n=z^{n+1}$ tiene una infinidad de soluciones. Sugerencia: considerar $[a(a^n+b^n)]^n+[b(a^n+b^n)]^n$.

40. Mostrar que si $n \in \mathbb{Z}$, entonces $3n^2-1$ no es un cuadrado.

41. Sea $a>1,\ t\neq 0$. Mostrar que $\operatorname{mcm}(a,a,ta)\operatorname{mcd}(a,a,ta) \neq |a^3t|$. Concluir que el Corolario 4.4 no es válido para 3 enteros.

42. Sean $a,b \in \mathbb{Z}$ con $a\neq 0$. Mostrar que $a \mid b$ si y sólo si $\operatorname{mcd}(a,b)=|a|$.

43. Sea $m=|a_1a_2\cdots a_n|\neq 0$. Mostrar que:

$$m=\operatorname{mcm}(a_1,a_2,...,a_n)\operatorname{mcd}\left(\frac{m}{a_1},\frac{m}{a_2},...,\frac{m}{a_n}\right).$$

44. Sea $m>0$ un múltiplo común de $a_1,a_2,...,a_n$. Mostrar que:

$$m=\operatorname{mcm}(a_1,a_2,...,a_n) \quad \text{si y sólo si } \operatorname{mcd}\left(\frac{m}{a_1},\frac{m}{a_2},...,\frac{m}{a_n}\right)=1.$$

45. Mostrar que si $a\neq 0\neq b$ y $\operatorname{mcd}(a,b)=\operatorname{mcm}(a,b)$, entonces $|a|=|b|$.

46. Mostrar que si $a,b\in\mathbb{Z}$ y $k\in\mathbb{N}$ son tales que $a^k \mid b^k$, entonces $a \mid b$.

47. Sean $a_1,...,a_r \in \mathbb{N}$ tal que $\operatorname{mcd}(a_i,a_j)=1$ para $i\neq j$. Si $\prod_{i=1}^{r} a_i=c^m$, entonces $a_i=c_i^m$, para $1\leq i\leq r$.

48. Mostrar que no existen $x,y\in\mathbb{Z}$ tal que $x+y=100$ y $\operatorname{mcd}(x,y)=7$.

49. Mostrar que las ecuaciones $x+y=l$ y $\operatorname{mcd}(x,y)=g$ tienen solución común si y sólo si $g|l$.

50. Mostrar que el sistema de ecuaciones

$$\begin{aligned}\operatorname{mcd}(x,y) &= g\\ \operatorname{mcm}(x,y) &= l\end{aligned}$$

es soluble en los enteros x,y si y sólo si $g \mid l$.

51. Mostrar que si $a_1, ..., a_m$ son enteros y $m > 1$ con al menos un $a_i \neq 0$, existen $t_1, ..., t_m \in \mathbb{Z}$ tales que $\text{mcd}(a_1, ..., a_m) = a_1t_1 + ... + a_mt_m$.

52. Mostrar que si $\text{mcd}(a_1, b_1) = \text{mcd}(a_2, b_2) = 1$ y $\dfrac{a_1}{b_1} + \dfrac{a_2}{b_2} \in \mathbb{Z}$, entonces $|b_1| = |b_2|$.

53. Mostrar con un ejemplo que la afirmación: $\displaystyle\sum_{i=1}^{r} \frac{a_i}{b_i} \in \mathbb{Z}$ y $\text{mcd}(a_i, b_i) = 1$ implica que $|b_1| = ... = |b_r|$ no necesariamente es cierta si $r \geq 3$.

54. Mostrar que si $\text{mcd}(ab, m) = 1$, entonces $\text{mcd}(a, m) = \text{mcd}(b, m) = 1$.

55. Mostrar que $\text{mcd}(a, b) = 1$ y $3 \nmid a+b$ entonces $\text{mcd}(a+b, a^2-ab+b^2) = 1$.

56. Si p es primo impar y $x \in \mathbb{N}$, entonces $\text{mcd}\left(x-1, \dfrac{x^p-1}{x-1}\right) = 1$ o p.

57. Si p es primo impar y $x \in \mathbb{N}$, entonces $\text{mcd}\left(x+1, \dfrac{x^p+1}{x+1}\right) = 1$ o p.

58. Mostrar que si $\text{mcd}(a, b) = 1$ y p primo impar tal que $p \nmid a + b$, entonces

$$\text{mcd}\left(a+b, \frac{a^p+b^p}{a+b}\right) = 1.$$

59. Mostrar que $\text{mcd}(a^2, b^2) = \text{mcd}(a, b)^2$.

60. Si p es primo, ¿qué posibles valores toma $\text{mcd}(a, p)$?

61. Encontrar 765438 enteros consecutivos todos ellos compuestos.

62. Mostrar que el número 2003 es primo.

63. Definimos el n-ésimo número de Mersenne como $M_n = 2^n - 1$. Mostrar que si M_n es primo, entonces n es primo. Los números primos de esta forma son conocidos como primos de Mersenne[6]. Para más información sobre éstos números primos, el lector puede consultar el capítulo Hojas Sueltas.

64. Mostrar que si $2^n + 1$ es primo entonces n es potencia de 2. Los números primos de esta forma se conocen como primos de Fermat[7].

[6]Marin Mersenne (1588-1648). Teólogo franciscano y científico francés, íntimamente vinculado desde su juventud a Descartes, de cuyas doctrinas fue eficaz difusor a través del *círculo* de intelectuales constituído a su alrededor. Mantuvo relación con los más famosos sabios de su época y él mismo llevó a cabo notables investigaciones. Veía la doctrina cartesiana como el mejor antídoto contra deístas, libertinos y escépticos

[7]Pierre Fermat (1601-1665) nació en Beaumont-de Lomange Francia. Estudia leyes en Touluse y en sus ratos de ocio se dedica a la literatura y a las matemáticas. Contribuyó notablemente al desarrollo de la geometría analítica, el cálculo diferencial e integral, la teoría de números y la teoría de las probabilidades. Los principales escritos de Fermat fueron publicados por su hijo después de su muerte bajo el título *Varia Opera Mathematica*.

65. Si p es primo y $n \geq 2$, entonces $\sqrt[n]{p}$ es un número irracional.

66. Si p es primo y $n \leq -2$, entonces $\sqrt[n]{p}$ es un número irracional.

67. En general, el producto de dos números irracionales no necesariamente es irracional. Por ejemplo, si p es un primo, entonces $\sqrt{p}\sqrt{p} \in \mathbb{Z}$. Demostrar que si p_1, p_2 son primos diferentes, entonces $\sqrt{p_1 p_2}$ es un número irracional.

68. Sean p_1, p_2 números primos diferentes. Mostrar que $x^2 = p_1 p_2$ no tiene solución en $\mathbb{Q}$.

69. Si p_1, p_2 son primos diferentes, entonces $\sqrt{p_1}+\sqrt{p_2}$ es un número irracional.

70. Sean p_1, p_2 primos diferentes. Si $a, b \in \mathbb{Q}$ satisfacen $a\sqrt{p_1} + b\sqrt{p_2} = 0$, entonces $a = b = 0$. En el lenguaje del álgebra lineal el conjunto $\{\sqrt{p_1}, \sqrt{p_2}\}$ es $\mathbb{Q}$-linealmente independiente.

71. Mostrar que $\log_{10} 2$ es un número irracional.

72. Sean $a, n \in \mathbb{N}$ tal que $\sqrt[n]{a} \in \mathbb{Q}$. Mostrar que $\sqrt[n]{a}$ es un entero. Deducir que $\sqrt[3]{10}$ es un número irracional.

73. Mostrar que si $n \geq 2$, entonces $\sqrt[n]{n}$ es un número irracional.

74. Sean a, b números irracionales. ¿Puede ser que a^b sea racional? Sugerencia: Según el problema 65 $\sqrt{p}^{\sqrt{2}} = p^{-\frac{1}{2}}$ es irracional. Ahora considere los números $\sqrt{p}^{\sqrt{2}}$ y $\sqrt{2}$.

75. Sean $x, y \in \mathbb{R}$. Demostrar que $[x]+[y] \leq [x+y] \leq [x]+[y]+1$. Sea $n \in \mathbb{N}$ y $x \in \mathbb{R}$, ¿es posible dar una estimación para $[nx]$?

76. Sean $x \in \mathbb{R}$. Demostrar que:

$$[x] + [-x] = \begin{cases} 0 & \text{si } x \in \mathbb{Z} \\ -1 & \text{si } x \notin \mathbb{Z} \end{cases}$$

77. Sea $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ con $p_i \neq p_j$ $(i \neq j)$. Mostrar que la suma de todos los divisores positivos de n es $\prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$.

78. Sea $a = \prod_{i=1}^{r} p_i^{\alpha_i} (\alpha_i \geq 0)$ y $b = \prod_{i=1}^{r} p_i^{\beta_i} (\beta_i \geq 0)$. Entonces

$$\text{mcd}(a, b) = \prod_{i=1}^{r} p_i^{\mu_i} \quad \text{y} \quad \text{mcm}(a, b) = \prod_{i=1}^{r} p_i^{\gamma_i},$$

donde $\mu_i = \min\{\alpha_i, \beta_i\}$ y $\gamma_i = \max\{\alpha_i, \beta_i\}$.

79. Usar el problema anterior para verificar las siguientes relaciones:

    a) $\mathrm{mcd}(x, \mathrm{mcm}(y,z)) = \mathrm{mcm}(\mathrm{mcd}(x,y), \mathrm{mcd}(x,z))$.

    b) $\mathrm{mcm}(x, \mathrm{mcd}(y,z)) = \mathrm{mcd}(\mathrm{mcm}(x,y), \mathrm{mcm}(x,z))$.

    c) $\mathrm{mcd}(\mathrm{mcm}(x,y), \mathrm{mcm}(x,z), \mathrm{mcm}(y,z)) =$
    $\mathrm{mcm}(\mathrm{mcd}(x,y), \mathrm{mcd}(x,z), \mathrm{mcd}(y,z))$.

    d) $\mathrm{mcm}(x,y,z)\,\mathrm{mcd}(x,y,z) \leq |xyz|$. La igualdad se obtiene si y sólo si x, y, z son primos relativos por pares.

80. Mostrar que existe una infinidad de primos de la forma $4n+1$ y $4n+3$.

81. Para $x > 0$ sea $\pi(x) =$ el número de primos p tal que $p \leq x$. Así, $\pi(4) = 2$, $\pi(9) = 4$, etc. Se sabe que para $x \in \mathbb{N}$, $\pi(x) \geq \dfrac{\log x}{2 \log 2}$. Usar la desigualdad anterior para mostrar que el n-ésimo primo p_n obtenido en la criba de Eratóstenes satisface $p_n > 2^{2^n}$. También se puede hacer una prueba usando inducción y sin hacer uso de la desigualdad $\pi(x) \geq \dfrac{\log x}{2 \log 2}$.

82. *Postulado de Bertrand*. En 1845 el matemático francés Joseph Bertrand verificó que para cada entero n entre 2 y $3 \cdot 10^6$ existe al menos un primo entre n y $2n$. Este resultado, en forma general, es conocido como el *Postulado de Bertrand* y fue demostrado por Chebyshev en el año 1850 [15]. Supongamos cierto el *Postulado de Bertrand*. Mostrar que si p_n es el n-ésimo primo, entonces $p_n \leq 2^n$. Comparar con el problema anterior.

83. Consideremos la sucesión de números $2^{2^n} + 1$ con $n \in \mathbb{N}$. Probar que:

    a) Si $n < m$, entonces $2^{2^n} + 1$ es divisor de $2^{2^m} - 1$.

    b) Si $n \neq m$, entonces $\mathrm{mcd}(2^{2^n} + 1, 2^{2^m} + 1) = 1$.

    c) Usar b) para mostrar que existe una infinidad de números primos.

84. Mostrar que si $d \mid n$, entonces $2^d - 1 \mid 2^n - 1$.

85. Mostrar que si $a \in \mathbb{Z}$ y $a \neq 0$, entonces las únicas soluciones racionales de la ecuación $x^m = a$ son necesariamente enteras.

86. El n-ésimo número triangular lo definimos como $t_n = \dfrac{n(n+1)}{2}$, donde $n \in \mathbb{N}$. Demostrar que:

    a) La suma de cualesquiera dos números triangulares consecutivos es un cuadrado.

    b) Cualquier número de la sucesión $21, 2211, 222111, \ldots$ es triangular.

87. Demostrar que cualquier número de la sucesión $100001, 10000100001, ...$ es un número compuesto.

88. Supongamos que existe un número finito de primos $p_1, p_2, \ldots, p_n$. Usar el número $N = p_2p_3 \cdots p_n + p_1p_3 \cdots p_n + \ldots + p_1p_2 \cdots p_{n-1}$ para dar otra demostración acerca de la existencia de una infinidad de primos.

89. En 1953 el profesor John Thompson publica una variación de la prueba de Euclides acerca de la infinitud de primos [43]. Lo interesante de este trabajo es la posiblilidad de generar explícitamente nuevos primos a partir de una lista finita de ellos. Sean $2 = p_1 < p_2 < ... < p_n$ los primeros n números primos. Dividimos la lista anterior en dos subconjuntos $q_1, ..., q_r$ y $s_1, ..., s_t$. Sea $D = (q_1 \cdots q_r) - (s_1 \cdots s_t)$. Demostrar que:

    a) Existe un primo p tal que $p \mid D$ y $p \neq p_j$ para $1 \leq j \leq n$. Concluir que existe una infinidad de primos.

    b) Si $D < (p_n + 2)^2$, entonces D es un número primo.

    c) Usar el inciso b) con la lista $2, 3, 5, 7, 11, 13$ y con diferentes particiones. ¿Siempre se obtiene un número primo?

    d) Consideremos simplemente que $p_1 < p_2 < ... < p_n$ son n números primos diferentes. ¿Siguen siendo válidas las afirmaciones a) y b)?

90. En el análogo geométrico de la criba de Eratóstenes proporcionamos una familia de rectas con ciertas propiedades. Encontrar una familia de rectas con propiedades similares pero actuando en el semiplano de la izquierda.

91. Mostrar que no existe un número primo de la forma $8^n + 1$.

92. Mostrar que cada entero de la forma $3n+2$ tiene al menos un factor primo de la misma forma.

93. Mostrar que el único número primo de la forma $n^3 - 1$ es 7.

94. Si p es un número primo y $p \mid a^n$, entonces $p^n \mid a^n$.

95. Demostrar que cada entero $n > 11$ se puede escribir como suma de dos números compuestos.

96. Encontrar todos los números primos que dividen a 70!

97. Consideremos el conjunto $S = \{3n + 1 : n \in \mathbb{N}\}$. Un elemento de S lo llamaremos primo si no puede ser factorizado como producto de al menos dos elementos de S.

    a) Demostrar que cualquier elemento de S es primo o es un producto de primos.

    b) Con un ejemplo demostrar que existen elementos en S que tienen diferentes factorizaciones.

98. Encontrar los valores de n para los cuales $n^4 + 4$ es un número primo. Sugerencia: $n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2$.

99. Mostrar que si p es primo, entonces $p \mid n^p - n$ para todo $n \in \mathbb{Z}$.

100. Sean p, q primos diferentes. Entonces $\text{mcd}(p^n, q^m) = 1$ para $n, m \in \mathbb{N}$.

101. Mostrar que si p es primo y $p > 3$, entonces p es de la forma $6n \pm 1$.

102. Mostrar que si p es primo y $\text{mcd}(j, p) = 1$ entonces $\text{mcd}(kp + j, p) = 1$ para todo $k \in \mathbb{Z}$.

103. Mostrar que la única terna de números primos impares consecutivos es $3, 5, 7$. Concluir que el único número primo que es suma y diferencia de dos números primos es 5.

104. a) Sea $f(x) = x^2 + x + 11$. Verificar que $f(n)$ es un número primo para $n = 0, 1, ..., 9$ y $f(10)$ no es primo.

    b) Sea $f(x) = x^2 + x + 17$. Verificar que $f(n)$ es un número primo para $n = 0, 1, ..., 15$ y $f(16)$ no es primo.

    c) Acerca de la existencia de otros polinomios cuadráticos que representan algunos números primos, sugerimos al lector ver el bello artículo de Paulo Ribenboim [32].

105. Dos números primos $p < q$ se llaman primos gemelos si $q - p = 2$. No se sabe si existe una infinidad de ellos. Supongamos que $p < q$ son primos gemelos.

    a) Demostrar que los números 2027 y 2029 son primos gemelos.

    b) Demostrar que $pq + 1$ es un cuadrado perfecto.

    c) Demostrar que si $p > 3$, entonces $12 \mid p + q$.

106. Mostrar que no existe un polinomio $f(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$ tal que $f(n)$ es un número primo para toda $n \in \mathbb{N}$.

107. Sea $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ un polinomio no constante con coeficientes en $\mathbb{Z}$ y $a_0 \neq 0$. Mostrar que si $x_0 \in \mathbb{Z}$ es tal que $f(x_0) = 0$, entonces $x_0 \mid a_0$. Concluir que $f(x)$ tiene un número finito de raíces enteras. Si $a_0 = 0$ entonces ¿cómo se obtiene la misma conclusión?

108. Fermat observó que el problema de factorizar un entero impar n es equivalente a encontrar al menos una solución en los enteros x, y de la ecuación $n = x^2 - y^2$. Obviamente la solubilidad de la ecuación anterior produce factores de n. Consideremos $a, b, n \in \mathbb{N}$ tal que $1 < a < b < n$ y $n = ab$. Mostrar que si n es impar, entonces n se puede representar como una diferencia de dos cuadrados perfectos.

109. Mostrar que la ecuación $a^n + b^n = c^n$ no tiene soluciones enteras positivas con a y b impares y n par. Sugerencia: $a^n - 1 = (a^{\frac{n}{2}} - 1)(a^{\frac{n}{2}} + 1)$, donde los factores son números pares consecutivos, uno de ellos es divisible por 4.

110. Consideremos las matrices $M_{2\times 2}(\mathbb{Z}) = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} : a_i \in \mathbb{Z} \right\}$. Mostrar que la ecuación matricial $X^n + Y^n = Z^n$ tiene solución en $M_{2\times 2}(\mathbb{Z})$. ¿Se puede generalizar a matrices de tamaño $k \times k$?

111. Sean $a, b, m \in \mathbb{Z}$ tal que $\text{mcd}(a, b) = 1$ y $m \neq 0$. Mostrar que la sucesión $a + bk$ contiene una infinidad de números primos relativos con m.

112. Sea p un número primo que se puede escribir como la suma de dos cuadrados. Demostrar que p es de la forma $4n + 1$.

113. [Algoritmo de la División Modificado] En el Teorema 2.1 mostramos que si $a, b, \in \mathbb{Z}$ con $a \neq 0$, entonces existen enteros q y r únicos tal que $b = aq + r$ donde $0 \leq r < |a|$. El algoritmo de la división modificado lo establecemos como sigue: Sean $a, b, \in \mathbb{Z}$ con $a \neq 0$. Existen enteros q y r tal que $b = aq + r$ donde $0 \leq |r| < |a|$. Por ejemplo, si $a = 7$ y $b = 4$, entonces $b = 7 \cdot 0 + 4 = 7 \cdot 1 + (-3)$ con $|4|, |-3| < |7|$. Observamos que en este caso el cociente y el residuo no son únicos y sin embargo los residuos satisfacen que su valor absoluto es menor que $|a|$.

    a) Demostrar el algoritmo de la división modificado.

    b) Demostrar que el cociente y el residuo son únicos si y sólo si

    $$|a + b| \leq \max\{|a|, |b|\}.$$

    c) ¿Será cierta la siguiente versión del *algoritmo de la división* en $\mathbb{Z}$?: Sean $a, b, \in \mathbb{Z}$ con $a \neq 0$. Existen enteros q y r tal que $b = aq + r$, donde $0 \leq |r|^2 < |a|^2$. Si en lugar de usar $|\ |^2$ usamos $|\ |^n$ ¿qué sucede?

    d) ¿Se podrá calcular el mcd de dos enteros con alguno de los *algoritmos de la división* definidos anteriormente?

Bibliografía

[1] Alford W. R., Granville A., Pomerance C. *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), no. 3, 703-722.

[2] Apostol,T., *Calculus*, Volumen II, segunda edición, Reverté 1980.

[3] Clark, D.A., *A quadratic field which is euclidean but not norm-euclidean*, Manuscripta math. **83** (1994), 327-330.

[4] Crandall R., Pomerance C., *Prime numbers*, A computational perspecive. Springer Verlag, New York 2001.

[5] Derksen H., *The fundamental theorem of algebra and linear algebra*, American Mathematical Montly, **110** (2003), no. 7, 620-623.

[6] Dickson L. E., *History of the theory of numbers*, Vol. 1, Chelsea 1971.

[7] Ecker A., *On primitive roots*, Elem. Math. **37** (1982), no. 4, 103-108.

[8] Erdös P., *On the least primitive root of a prime p*, Bull. Amer. Math. Soc., **51** (1945), 131-132.

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

[10] *Euclid: the thirteen books of the ELEMENTS*, vol. 2 (books III-IX), second edition unabridged. Dover 1956, New York.

[11] Euler L., Elements of Algebra, Springer Verlag, New York 1984.

[12] Fine B., Rosenberg G., *The Fundamental Theorem of Algebra*. Springer-Verlag UTM, 1997.

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

[14] Gerstenhaber M., *The 152nd proof of the law of quadratic reciprocity*. American Mathematical Montly, **70** (1963), 397-398.

[15] Hardy G.H., Wright E.M. *An introduction to the theory of numbers*. Oxford University Press 1979.

[16] Hooley C., *On Artin's Conjeture*, reine angew. Math. **226** (1967), 209-220.

[17] Ireland K., M. Rosen., *A classical introduction to modern number theory*. GTM **84** Springer Verlag 1982.

[18] Jones J.P., *et al. Diophantine representation of the set of prime number*. American Mathematical Montly, **83** (1983).

[19] Kummer E.E., *Neuer elementarer Beweis, dass die Anzahl aller Primzahlen eine unendliche ist*. Monastber. Akad. d. Wiss., Berlin 1878 (**9**), 777-778.

[20] Kuratowski K., *Introducción al cálculo*. Limusa 1978, México.

[21] Kurosch, A.G., *Curso de álgebra superior*. Limusa-Mir 1994, México.

[22] Lenstra, H. W., Jr. *Solving the Pell equation*. Notices Amer. Math. Soc. **49** (2002), no. 2, 182-192.

[23] Lloyd M., Dybas H.S., *The periodical cicada problem*, Evolution **20** (1966), 466-505.

[24] Malcolm N., The publications of John Pell, F.R.S. (1611-1685): some new light and some old confusions. Notes and Records Roy. Soc. London **54** (2000), No.3 , 275-292.

[25] Mathews G.B., *Theory of Numbers*, Cambridge, 1892.

[26] Motzkin, Th., *The euclidean algorithm*. Bull. Amer. Math. Soc. **55** (1949).

[27] Murty M. Ram., *Artín conjeture for primitive roots*, Math. Intellingencer **10** (1988), No. 4, 59-67.

[28] Nagell T. *Number theory*. Chelsea 1964.

[29] Perlis R., *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), 342-360.

[30] Pohst M., Zassenhaus H., *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications, **30**. Cambridge University Press, Cambridge 1997.

[31] Ribenboim P., *Algebraic Numbers*, New York, Wiley 1972

[32] Ribenboim P., *El famoso polinomio generador de primos de Euler y el número de clase de los cuerpos cuadráticos imaginarios*. Revista Colombiana de Matemáticas, vol. **21** (1987), 263-284.

[33] Ribenboim P., *The new book of prime number records*. Springer Verlag, New York (1996).

[34] Morales Guerrero L.E., Rzedowski Calderón M., *Contando sobre números*. Avance y Perspectiva CINVESTAV-IPN vol. **18** (1999).

[35] Rivest R., Shamir A., Adleman L., *A method for obtain digital signatures and public-key cryptosystems*. Comm. of the ACM, **21**, 120-126 (1978).

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

[37] Singh S., *Fertmat's Enigma*. Penguin Books,1998.

[38] Stark M.H., *A complete determination of the complex quadratic fields of class-number one*. Michigan Math. J. **14** (1967) 1–27.

[39] Stark M.H., *A historical note on complex quadratic fields with class-number one*. Proc. Amer. Math. Soc. **21** (1969) 254–255.

[40] Stark M.H., *An introduction to number theory*. MIT Press (1978).

[41] Stewart I., Tall D., *Algebraic Number Theory and Fermat Last Theorem*. A K Peters, third edition, 2002.

[42] Tenenbaum G., France M.M., *The Prime Numbers and Their Distribution*. Student Mathematical Library (AMS), vol. **6** (2000).

[43] Thompson J., *A method for finding primes*. American Mathematical Monthly, **60**, No. 3, 175 (1953).

[44] Weil A., *Two lectures on number theory, past and present*, Enseignement Math. **20** (1974), 87-110.

[45] Weil, A., *Oeuvres Scientifiques, Collected Papers*, vol. **III**, pp 398-403. Springer-Verlag (1979), New York.

[46] Zaldivar Cruz F., *La función zeta de Riemann*. Miscelánea Matemática (SMN), No. **36** (2002).