Agradecimiento

Al Departamento de Matemáticas de la Facultad de Ciencias, Universidad de Los Andes, por haberme respaldado en esta tarea de redactar el presente libro de texto.

A mis colegas del grupo de álgebra: Los Dres. Joaquín Pascual y José Rodríguez, por su paciencia y dedicación puesta de manifiesto en la corrección del manuscrito original, así como también por sus valiosas sugerencias sobre la forma de presentación del material. Gracias también al profesor Aristides Arellán.

Al Br. Angel Pérez por su valiosa ayuda en la dactilografía del texto.

Al Consejo de Desarrollo Científico y Humanístico de la Universidad de los Andes por haber financiado parte de este trabajo.

Contenido

Introducción

La teoría de números es la rama de las matemáticas que estudia las propiedades aritméticas de los números enteros. Propiedades aritméticas son todas aquellas que tienen que ver con suma y producto de números. Por ejemplo, dado un número entero n, el problema de hallar todos sus divisores es un problema típico de la teoría de números. En esta introducción haremos una exposición, desde el punto de vista histórico, de cómo se ha desarrollado esta disciplina, concentrándonos en los hechos más importantes y en sus protagonistas. Es una historia muy larga, tan larga como la del hombre, pero nos enseña comó el hombre se ha planteado problemas difíciles desde el punto de vista teórico y cómo se han resuelto estos problemas con la introducción de nuevas ideas y métodos de razonamiento. Estas nuevas rutas han generado un panorama inmenso dentro de la matemática actual, debido a una evolución lenta, pero extraordinaria, del pensamiento de todos estos hombres.

Epoca Antigua

El origen de la teoría de números se remonta a los orígenes de la civilización, con los habitantes de Caldea y Babilonia hace 3500 años aproximadamente. Ellos han dejado sus conocimientos escritos en símbolos cuneiformes, los cuales han llegado bastante bien conservados hasta nuestros días. En algunas de estas tablillas se han calculado soluciones enteras de la ecuación

$$a^2 + b^2 = c^2$$

Como por ejemplo el triple (3, 4, 5), el cual satisface: $3^2+4^2 = 5^2$. Los babilonios conocían ésta y otras soluciones y nos dejaron una lista de más de sesenta de ellas. Sin embargo no se conoce el método empleado por ellos para llevar a cabo estos cálculos.

Con los griegos aparecen las primeras demostraciones formales en matemática, lo cual es un avance extraordinario en comparación con las culturas anteriores. Antes de ellos, los problemas se resolvían de

manera particular sin dar un método general para hallar las soluciones. El espíritu de razonamiento griego, claro y riguroso, establece las bases sobre las que se ha desarrollado la matemática a través de los siglos.

Una muestra de esta capacidad de razonamiento abstracto de los matemáticos griegos son todos esos hermosos teoremas sobre geometría plana, en donde se demuestran de forma elegante, proposiciones sobre áreas de triángulos, cuadrados y polígonos, usando propiedades muy simples sobre puntos, intersección de líneas, etc.

Así vemos como **Pitágoras** (500 a.c.) nos da un método general para hallar todas las soluciones de la ecuación

$$x^2 + y^2 = z^2$$

razón por la cual, se le da el nombre de Ecuación Pitagórica.

Aparte de Pitágoras, hay que mencionar a otros dos grandes matemáticos griegos, cuya contribución a la teoría de números es muy importante.

El primero de ellos es **Euclides** (300 a.c.) quien escribió uno de los libros más famosos que se conoce sobre Geometría, llamado *Los Elementos*. Este libro es un modelo del método de demostración creado por los griegos, llamado método deductivo, mediante el cual se demuestran teoremas y proposiciones a partir de otras proposiciones simples llamadas axiomas , en forma lógica y muy eficiente.

En uno de estos elementos, Euclides establece una serie de proposiciones sobre los números enteros, las cuales pueden ser consideradas como el inicio de la teoría de números. Por ejemplo, la prueba sorprendente de que existe un número infinito de números primos.

Euclides suponía que existe un número finito de primos $p_1, p_2, \ldots, p_t$, luego el número

$$x = p_1 p_2 \ldots p_t + 1$$

no está en la lista de los anteriores y por lo tanto, no es primo.

Sin embargo, usando el teorema de Factorización única de los números enteros, el cual se debe también a Euclides, se concluye que x

tiene algún divisor primo p_i . Esto nos lleva a una contradicción, pues p_i no puede dividir a $p_1 p_2 \dots p_t + 1$.

Este método de demostración, llamado reducción al absurdo, se debe a los griegos y ha sido uno de los más utilizados en la matemática desde entonces.

Los números primos: 2, 3, 5, 7, ... han ejercido una atracción fascinante sobre todos los matemáticos desde la época de los griegos. Su distribución en el conjunto de los enteros es realmente un misterio, por la forma tan irregular como aparecen. Ellos han ocupado un papel de primera importancia dentro de la teoría de números; muchas preguntas sobre los números primos, aún hoy en día, permanecen sin respuesta.

También a Euclides se debe el algoritmo para hallar el máximo común divisor entre dos enteros, el cual es una aplicación del teorema de la división. Gracias a este algoritmo, y al teorema de factorización única, se pueden obtener muchas propiedades importantes sobre la aritmética de los enteros.

El tercer matemático griego cuya contribución a la teoría de números ha sido fundamental, fue **Diofantos de Alejandría** (250 a.c.); llamado el Padre de la Teoría de Números.

Diofantos escribió muchos libros de matemática (cerca de 12), de los cuales sólo han sobrevivido cuatro. El más importante de todos es *La Aritmética*.

Esta obra es un tratado de resolución de ecuaciones algebráicas provenientes de la solución de problemas prácticos. El método empleado por Diofantos en el tratamiento de estas ecuaciones, consiste en hacer cambios de variable muy ingeniosos para reducir el grado de éstas, así como el número de indeterminadas. Los problemas planteados son en números enteros, de cierta dificultad, y llegan a aparecer ecuaciones hasta de sexto grado con varias variables. Por ejemplo en el libro IV aparecen las ecuaciones

$$x^2 + 2 = u^3$$

$$x^2 - 4x + 4 = u^3$$

También ecuaciones más complejas con tres incógnitas, como

$$\left(\sum_{i=1}^{3} x_i\right)^3 + x_k = u_k^3 \quad k = 1, \ldots, 3$$

En la mayoría de los casos, Diofantos obtiene una solución particular de los problemas, sin demostrar un método general. Cada ecuación es tratada individualmente haciendo uso de brillantes artificios de cálculo. Sin embargo, se sabe que muchos de los problemas planteados poseen otras soluciones de las cuales él no estaba consciente.

No obstante, Diofantos menciona tres lemas en su Aritmética, llamados Porismos, que quizás fueron demostrados. Uno de ellos dice:

Si $x + a = u^2$ e $y + a = v^2$, $xy + a = w^2$, entonces $v = u + 1$.

También se puede concluir que Diofantos conocía algunos hechos importantes de la teoría de números, pero cuya demostración se produjo varios siglos más adelante. A manera de ejemplo, Diofantos conocía :

1. Todo primo de la forma 4n + 1 es suma de dos cuadrados.

2. Ningún primo de la forma 4n + 3 es suma de dos cuadrados.

3. Ningún número de la forma 8n + 7 es suma de tres cuadrados.

4. Todo entero positivo es suma de cuatro cuadrados.

Todos estos problemas fueron atacados por los matemáticos de épocas posteriores y algunos de ellos fueron resueltos en el siglo XVIII.

Otro aporte muy valioso de Diofantos fue el estudio de los números poligonales. Un número es poligonal cuando representa la suma de los puntos enteros dentro de un polígono. Por ejemplo, los números triangulares son 1, 3, 6, 10, ... etc. Diofantos obtuvo una fórmula para hallar todos los números poligonales.

La obra de Diofantos ciertamente dio inicio a la teoría de números. Sin embargo no fue apreciada en toda su magnitud por los matemáticos posteriores. Transcurren varios siglos sin haber algún hecho importante

en esta área de la matemática, después del impulso vigoroso dado por los griegos. Hubo de esperar hasta el siglo XVII cuando Pierre de Fermat y otros, descubren las viejas traducciones de su obra y aprecian el verdadero valor de sus ideas.

Apartándonos un momento de la Civilización Occidental, volvamos nuestra mirada hacia la antigua China, en donde la matemática ha alcanzado un cierto desarrollo durante la Edad Media, independientemente de Occidente.

Una figura de gran relevancia en este ambiente, es sin duda el matemático, poeta y arquitecto **Ch'in Chiu-Shiao** (1202 d.c.), cuya obra más importante es el libro *Shu-shu chiu-chang* (Tratado de Matemáticas).

Dicha obra esta dividida en nueve secciones:

1. El análisis indeterminado.
2. Calendario astronómico y cálculos metereológicos.
3. Agrimensuría.
4. Métodos de triangulación en la agrimensuría.
5. Impuesto a las propiedades.
6. Economía.
7. Asuntos militares.
8. Compras y ventas.
9. El comercio de trueque.

Por esta lista tan diversa de tópicos, podemos darnos una idea del avance de la matemática en China y sus aplicaciones en aquella sociedad. Sin embargo, la parte que nos interesa es el Análisis Indeterminado en cuyo texto se exponen problemas matemáticos que conducen a sistemas de ecuaciones de congruencia. Estos problemas tienen una

data muy antigua como el siguiente, que apareció en un libro de Chin en el siglo IV d.c.

Existe una cantidad de cosas que al contarlas de tres en tres, deja un residuo de dos; al contarlas de cinco en cinco deja un residuo de tres; al contarlas de siete en siete deja un residuo de dos. Hallar el número de cosas.

Este problema se puede plantear usando la notación de congruencias

$$x \equiv 2 \ mod \ 3$$
$$x \equiv 3 \ mod \ 5$$
$$x \equiv 2 \ mod \ 7$$

donde x es la cantidad de cosas.

Este es un caso especial del Teorema chino del resto, y Shao nos da la solución $x = 23$, la cual se obtiene mediante un algoritmo desarrollado por él. No se sabe si los chinos conocían el método general para resolver este tipo de problemas.

En el año 622 se inicia la expansión del imperio árabe, cuya hegemonía en Europa duró cerca de ocho siglos. En pocos años, los árabes tomaron las ciudades de Damasco y Jerusalem. En 1641 se produce la toma de Alejandría, que era el centro cultural y científico más importante de la antiguedad.

Los árabes no tenían al comienzo una cultura matemática propia, pero se dedicaron a traducir obras de los griegos, persas e hindúes a fin de asimilar esos conocimientos. Por ejemplo, de los indúes tradujeron el *Surya Siddhanta* y de los griegos el *Almagest* de Ptolomeo y *Los Elementos* de Euclides.

Hacia el año 800, el centro cultural de este imperio era Bagdad, en donde el Califa Al-Manun fundó una casa de sabiduría, la cual era centro de reunión de matemáticos y astrónomos. Uno de estos, **Mohamed ibn-Musa al-Khowarizmi**, se convertiría en el más famoso de todos los matemáticos árabes; siendo su influencia tan grande como la de Euclides entre los griegos.

Este matemático escribió cerca de 6 obras de álgebra y astronomía; la primera de ellas inspirada en el libro *Sindhind* de los hindúes. Su interés por la ciencia fue muy amplio pues, aparte de matemáticas y astronomía, escribió sobre astrolabios, relojes de sol y geografía. En uno de sus libros titulado *El arte de contar* se hace una exposición completa del sistema de numeración en base 10, sistema este que fue inventado por los hindúes. Dicho sistema se conoció en Europa gracias a los escritos de al-Khowarizmi, razón por la cual algunos le atribuyen a los árabes la invención de nuestro sistema de numeración actual, llamado sistema arábigo o decimal.

La palabra algorismo, empleada a partir de los árabes, en relación con las operaciones de suma y multiplicación en base 10, proviene del nombre de al-Khowarizmi.

El libro más difundido de al-Khowarizmi fue el *Al-jabr wa'l*, palabra ésta que dio origen al término álgebra. Este texto fue muy conocido en Europa y contribuyó a dar a conocer el álgebra entre los matemáticos medievales, razón por la cual se llama a al-Khowarizmi el Padre del Algebra.

Comienza este maravilloso libro con una exposición de las principales propiedades de los números enteros y fraccionarios. Luego resuelve muchas ecuaciones, en donde intervienen raíces cuadradas y potencias. Es importante mencionar la forma rigurosa y exhaustiva cómo trabaja este autor, resolviendo todos los casos posibles de ecuaciones lineales y cuadráticas en una incógnita.

También contiene muchas demostraciones geométricas de ecuaciones algebráicas, usando el método desarrollado por los griegos, el cual consistía en asociar a un número la longitud de un segmento lineal y al cuadrado de un número el área de un cuadrado.

Hacia la postrimerías de la Edad Media, otro matemático árabe **Al-Kashi** produce uno de los libros más completos de matemática elemental de la antiguedad. Esta verdadera enciclopedia, llamada *Miftah al-Hisab*, estaba destinada al uso de calculistas , arquitectos , agrimensores y comerciantes. En la parte de álgebra se destacan las fórmulas para elevar un binomio a cualquier potencia (Binomio de Newton).

También se da la construcción de los coeficientes binomiales a través del triángulo de Pascal.

En otro de los libros se estudia la teoría de ecuaciones algebráicas de grado menor o igual a cuatro. Al-Khashi obtuvo fórmulas para resolver algunas ecuaciones de cuarto grado, lo cual es realmente sorprendente para su época. Anteriormente, otro matemático árabe, **Omar al-Khayyami** había descubierto fórmulas para resolver la ecuación cúbica.

Con al-Khashi se cierra el ciclo de la matemática arábiga. Después de su muerte en 1436 el imperio musulmán comienza a desintegrarse y desaparece del panorama europeo. A partir de allí comienza una nueva corriente de la matemática, con el renacimiento, en donde comienzan a profundizarse los métodos del álgebra, motivado por la resolución de ecuaciones de grado mayor que tres.

Si bien la teoría de números no muestra ningún avance importante en este período; este desarrollo del álgebra y la geometría preparará el camino para los grandes pasos que se darán en el siglo XVII.

Epoca Moderna

Iniciando la nueva era de la matemática moderna, encontramos la figura de **Pierre de Fermat** (1601-1665) , sin duda el más grande de los matemáticos del siglo XVII en el área de teoría de números. Es en este siglo cuando se presencian los mayores avances en casi todas las áreas de matemática, con la invención del cálculo por parte de Issac Newton y Leibniz , y por otra con el descubrimiento de la geometría analítica por Descartes y el mismo Fermat.

Se conocen pocos hechos acerca de la vida privada de Fermat, quién nació en Beaumont-de-Lomagne en Francia el 20 de Agosto de 1601. Proveniente de una familia con buena posición económica, Fermat se dedicó a estudiar leyes y obtiene la licenciatura en 1631. Luego se instala en la ciudad de Tolouse en donde ejerce el cargo de Consejero del Parlamento local. Debido a esto, disponía de tiempo suficiente para dedicarse al estudio de las obras clásicas de la literatura y la

matemática. Tenía un gran dominio de las lenguas: francés, italiano, español, latín y griego. También demostró cierta inclinación hacia la poesía, componiendo versos en latín.

Durante su época de estudiante en Bordeaux volcó su atención hacia la matemática, al estudiar en profundidad la obra de **Francisco Vieta**, quien fue el más grande algebrista del siglo XVI. Vieta desarrolló la notación simbólica del álgebra, lo cual facilitó considerablemente el manejo de las variables dentro de una ecuación. Fermat retoma las ideas de Vieta sobre el tratamiento analítico, de muchos problemas planteados por los antiguos de Algebra y Geometría. La teoría de ecuaciones de Vieta, en donde se analizan las relaciones entre las distintas soluciones de una ecuación y la estructura de las mismas, permitió a Fermat desarrollar un nuevo método llamado *Análisis Reductio*. Con esta herramienta resuelve muchos problemas geométricos de Pappus y Apolonio, sobre construcciones con regla y compás, planteando ecuaciones algebráicas en una variable real.

Fermat estudió profundamente la obra de Diofantos, Euclides y Apolonio, se interesó en los problemas planteados por ellos e intentó resolverlos usando los métodos modernos. Este nuevo enfoque fue muy fructífero para la teoría de números, pues Fermat pudo hallar soluciones muy generales para muchas ecuaciones Diofánticas, usando métodos de demostración suficientemente rigurosos.

Muchos de los resultados de Fermat han llegado hasta nosotros por las anotaciones que hacía sobre el margen de la Aritmética de Diofantos, traducida por el matemático Bachet. También tuvo una extensa correspondencia con otros matemáticos de su época como Mersenne, Frenicle, Pascal y Carcavi, a quienes les formulaba problemas difíciles de teoría de números a manera de reto.

El interés de Fermat en teoría de números no tenía límites: se ocupaba de los números primos, números amigables, sumas de cuadrados, ecuaciones de congruencias y otras cuestiones relacionadas con la aritmética de los enteros.

Demostrando una sagacidad muy superior a la de todos los matemáticos que le precedieron, Fermat descubrió y enunció el siguiente

resultado, muy importante

Si p es un número primo, entonces

$$a^{p-1} \equiv 1 \; mod \; p$$

Este resultado, conocido como el pequeño teorema de Fermat, nos da el primer test de primalidad conocido para un número p. Hoy en día se conoce una generalización de este resultado en la teoría de grupos.

La intuición de Fermat para plantear problemas en teoría de números, es realmente maravillosa. Algunos de estos problemas los resolvió usando sus propias técnicas, otros, sin embargo, fueron resueltos por matemáticos de siglos posteriores despúes de haber sido atacados por los mejores hombres de ciencia de varias épocas.

Veamos algunos de ellos, propuestos en varias cartas a Carcavi

1. Todo número primo de la forma 4n+1 se puede escribir como suma de dos cuadrados.

2. Todo número natural se expresa como suma de cuatro cuadrados.

3. La ecuación
$$x^2 - dy^2 = 1$$
tiene infinitas soluciones.

Fermat halló demostraciones correctas para los problemas 1) y 3), sin embargo no pudo hallar una demostración general para el 2). Este fue resuelto dos siglos después por Lagrange.

El problema más famoso planteado por Fermat, quizás el más famoso de toda la matemática, es el **Gran Teorema de Fermat**. Este consiste en probar que la ecuación

$$x^n + y^n = z^n$$

no posee solución para x, y, z números enteros, si $n \geq 3$.

Para n=2, esta ecuación se reduce a la ecuación pitagórica, de la cual ya hemos hablado.

Fermat dijo que él tenía en su poder una prueba maravillosa de tal teorema, pero nunca la dejó escrita. Muchos matématicos dudan que esto sea cierto debido a la dificultad del teorema, por una parte, y porque Fermat dio una demostración para el caso particular $n = 4$, de la cual se sentía muy orgulloso, en donde desarrolla un nuevo método de prueba llamado *Descenso al Infinito*.

El Teorema de Fermat ha llamado poderosamente la atención de los mejores matemáticos de todas las épocas. Si bien ha sido atacado durante más de tres siglos no ha podido resolverse completamente. En los intentos por hallar una solución a este misterio se ha producido mucha matemática, con la aparición de nuevas técnicas muy sofisticadas, como lo son la teoría de números algebráicos y la geometría algebráica, entre otras.

La demostración del caso $n = 3$, descubierta por Euler un siglo más tarde, es muy complicada y utiliza técnicas desconocidas para la época de Fermat.

En 1847, **E. Kummer** probó que el teorema de Fermat es cierto para todo $n \leq 100$. Recientemente, en 1977, S.S. Wagstaff usando métodos de computación, probó que el teorema es cierto para todo primo p , con $p \leq 125.000$. Finalmente, hay que mencionar a Andrew Wiles quien en 1993 parece haber hallado una demostración de dicho teorema.

Después de Fermat, la teoría de números permaneció sin muchos progresos por un siglo, hasta la llegada del gran matemático suizo **Leonhard Euler**, quien nació en 1707 en Basilea. A la edad de 14 años, ingresa a la Universidad de Basilea, en donde recibe clases del célebre matemático Johan Bernoulli I. Demostrando su genialidad desde temprana edad, publica su primer resultado sobre matemáticas a los 18 años.

En 1726 es llamado a la Academia de San Petersburgo, donde se le ofrece un cargo de profesor. Allí, además de enseñar matemáticas,

investiga mucho en ciencias aplicadas como física, ingenieria, navegación, construcción naval y cartografía. Luego, en 1741, se traslada a la Academia de Ciencias de Berlín, invitado por el Rey Federico el Grande de Prusia. En esta academia permaneció hasta 1766 cuando la Reina Catalina II de Rusia lo llama nuevamente a la Academia de San Petersburgo, donde permanece hasta su muerte en 1783.

La vida de Euler fue una de las más fructíferas que haya tenido matemático alguno. Fue un escritor infatigable: ¡su obra completa alcanza más de 70 volúmenes! Lo más asombroso es la gran cantidad de artículos escritos en los últimos diez años de su vida cuando estaba ciego. Además de estos artículos, Euler escribió un libro llamado *Introducción al Análisis Infinito* que se puede considerar como el primer libro del análisis moderno y que tuvo mucha influencia en la evolución de la matemática posterior a él.

Gracias a Euler tenemos la notación moderna que utilizamos hoy en día en: series, números complejos, sumatorias potencias, exponenciales y muchas funciones de la matemática. Euler recopiló todos los resultados que se conocían en teoría de números, que se hallaban dispersos en cartas y pequeños artículos, dándoles una nueva apariencia con las notaciones modernas.

En el campo de la teoría de números, Euler inició una nueva etapa en esta área, al probar algunos teoremas usando métodos del análisis. Esta nueva rama iniciada por Euler se conoce con el nombre de teoría analítica de números. A manera de ejemplo, mencionaremos su demostración de la infinitud de los números primos, la cual se basa en demostrar que la serie

$$\sum \frac{1}{p}$$

diverge, donde p recorre el conjunto de los números primos.

Es importante destacar la labor realizada por Euler, al continuar la obra de Fermat, resolviendo algunos problemas difíciles planteados por este último. Así pues, Euler probó en forma general el pequeño teorema de Fermat, el cual ya hemos mencionado, y además dio un resultado

mucho más general, para lo cual introdujo una nueva función en los números enteros. Si n es un entero positivo, entonces la función ϕ de Euler, aplicada a n, es un número entero positivo $\phi(n)$ el cual es igual al número de enteros x, $1 \leq x < n$ que son primos relativos con n. El teorema del cual hablamos, llamado Teorema de Euler, establece

$$a^{\phi(n)} \equiv 1 \ mod \ n$$

para todo entero a.

Euler poseía una capacidad de cálculo extraordinaria, muy superior a la de cualquier matématico de su época. Fermat había supuesto que todo número de la forma

$$2^{2^n} + 1$$

siempre es primo, para cualquier n.

Este resultado lo comprobó el mismo Fermat, para los valores de $n = 1, 2, 3, 4$. Sin embargo Euler probó que para $n= 5$ el resultado es falso, mostrando la factorización

$$2^{2^5} + 1 = 4.294.967.297 = 6.700.417 \times 641$$

resultado este, que habla por si sólo de las habilidades de Euler para factorizar números compuestos bastante grandes.

Durante el siglo XVIII, gracias a la obra de Euler y los hermanos Bernoulli, la matemática demostró su poder de aplicación a otras ramas de la ciencia como la astronomía, mecánica, hidráulica,...etc. Uno de las figuras más importantes en este período fue **Joseph Louis Lagrange**, de quien se puede afirmar, a través de sus obras, fue el más grande de los matemáticos del siglo XVIII.

Lagrange nace en Turín, Italia en 1736 y muere en Francia en 1813. Desde joven se interesó en las lenguas clásicas: latín y griego, pero también tuvo un fuerte interés en la matemática, razón por la cual, lo vemos como profesor de Artillería en Turín a los 19 años de edad. En 1766, ayudado por d'Alembert, obtiene un puesto en la Academia de Berlín, hasta 1787 cuando ingresa a la Academia Francesa en París donde permaneció hasta su muerte en 1813.

La obra de Lagrange está claramente marcada en estos tres períodos en donde fijó su residencia. Los dos primeros períodos; el de Turín y Berlín, fueron de mucha actividad científica. Comenzando en 1745 con el descubrimiento del cálculo de variaciones y la posterior aplicación de este a la mecánica en 1756. El también trabajó en mecánica celeste en esta época, estimulado por los concursos de la Academia de Ciencias de París.

En 1762 se establece una competencia científica, cuando la Academia formula la siguiente pregunta: ¿ Cómo se puede explicar físicamente que La Luna siempre presenta la misma cara hacia La Tierra? En 1763 Lagrange envía una memoria a la Academia titulada " *Investigaciones sobre la liberación de La Luna, en donde se ataca el problema propuesto por la Real Academia de Ciencias*". En este trabajo, Lagrange da una explicación satisfactoria sobre los movimientos de La Luna.

Más tarde en 1766 la misma Academia propone otra pregunta: ¿Como se explica matemáticamente, el movimiento de los cuatro satélites de Júpiter? Nuevamente Lagrange envía una memoria, dando una explicación correcta de este hecho y la cual resultó ganadora del concurso.

Durante su estadía en Berlín en 1770, Lagrange expone ante la Real Academia uno de sus mejores resultados en teoría de números: *Demostración de un teorema de aritmética*, en donde demuestra un problema que había sido planteado por Fermat, y atacado por Euler y otros matemáticos sin ningún éxito. El problema consiste en probar: Todo número natural puede ser representado como suma de cuatro cuadrados.

En esta misma línea de investigación, aparece en 1771 una demostración de un teorema propuesto por Wilson :

p es un número primo si y sólo si $(p-1)!+1$ es un múltiplo de p.

Finalmente mencionaremos los trabajos de Lagrange sobre la Ecuación de Fermat (o Ecuación de Pell)

$$x^2 - dy^2 = 1$$

Lagrange da una prueba completa de que esta ecuación posee infinitas soluciones, para lo cual desarrolla toda la Teoría de Fracciones Continuas, que había sido iniciada por Euler. Esta ecuación posee un grado de dificultad superior a las otras ecuaciones diofánticas, tratadas por Fermat y Euler. Si esta ecuación se factoriza, entonces tendremos

$$(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$$

lo cual plantea la necesidad de trabajar con números de la forma $a + b\sqrt{d}$, los cuales eran un misterio para los matemáticos de la época.

Si el par (x, y) es solución y además x e y son suficientemente grandes, entonces el cociente x/y es una aproximación de $\sqrt{d}$. El método de aproximación de numeros irracionales mediante una fracción continua, nos proporciona todas las soluciones de la ecuación de Fermat, esto lo demuestra Lagrange en su trabajo. Los métodos usados por Lagrange, la forma de escribir las demostraciones en forma clara y concisa, y el empleo de una lógica rigurosa hacen de este artículo una de las páginas más brillantes en toda la teoría de números.

Los años que Lagrange pasó en París, fueron dedicados a la docencia, escritura de obras didácticas y la publicación de grandes tratados de matemática. Todo esto contribuyó a darle a esta ciencia una nueva visión, a partir del siglo XIX. Lagrange tuvo una participación muy activa en todas las reformas científicas y educativas que se originaron durante la Revolución Francesa.

En Mayo de 1790, la Asamblea Constituyente decretó la unificación del sistema de pesas y medidas, y le dio a la Academia de Ciencias la tarea de buscar un sistema con una base única y que sería usado por todos los pueblos de la humanidad. Esta comisión, en la cual estaba Lagrange junto con otros científicos notables de la época, propuso el sistema de pesos y medidas en base 10, o decimal, el cual utilizamos en la actualidad.

Lagrange fue uno de los fundadores de la Escuela Normal y de la Escuela Politécnica de París, las cuales existen hoy en día. Estos dos centros han dado grandes aportes en el campo de la matemática, tanto en el siglo pasado como en el actual.

Uno de los matemáticos contemporáneos de Lagrange, cuya obra tuvo mucha influencia en el desarrollo posterior de la teoría de números, fue **Adrien-Marie Legendre** (1752- 1833). En 1782 ganó el premio de la Academia de Berlín con una memoria sobre balística. Esta trabajo llamó la atención de Lagrange, quien se interesó de inmediato en la obra de este joven matemático.

Legendre trabajó en las áreas de funciones elípticas, mecánica celeste y teoría de números. En 1798 publicó un obra titulada *Ensayo sobre la teoría de números* en donde aparecen una serie de resultados importantes, sobre la representación de un número primo por una forma cuadrática del tipo : $x^2 + ay^2$. En este trabajo se establece por vez primera la famosa *Ley de Reciprocidad Cuadrática*, la cual fue probada en forma definitiva por Carl. F. Gauss.

Si p es un número primo y a es un entero positivo, entonces Legendre define el símbolo: $\left(\frac{p}{a}\right)$ llamado símbolo de Legendre, el cual es igual a 1, si a es un residuo cuadrático módulo p, y -1 en el caso contrario. La ley de reciprocidad cuadrática establece entonces:

Si p y q son dos números primos, se tiene

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

Con el inicio del siglo XIX aparece la figura de uno de los matemáticos más grandes de todos los tiempos , quizás el más grande de todos, como lo fue el matemático alemán *Carl Friedrich Gauss* (1777-1855), llamado con justa razón: El Príncipe de los Matemáticos.

En 1795, bajo el patrocinio del Duque de Brunswick, entra en la Universidad de Götingen. El 30 de Marzo de 1796 a la temprana edad de 19 años, da muestra de su genio matemático al resolver uno de los problemas más antiguos (más de 2000 años) planteado por los matemáticos griegos, sobre la construcción de polígonos regulares con regla y compás. Gauss probó que se puede construir con regla y compás el polígono de 17 lados.

En forma más general, Gauss probó el siguiente resultado, usando las raíces de la ecuación

$$1 + x + x^2 + \ldots + x^{p-1} = 0$$

Se puede construir con regla y compás el polígono de n lados, si y solo si

$$n = 2^k p_1 \dots p_r$$

donde los p_i son primos de la forma

$$p_i = 2^{2^t} + 1$$

Unos días más tarde, el 18 de Abril de 1796, Gauss dio la primera prueba completa de la Ley de Reciprocidad Cuadrática, la cual había descubierto él mismo, independientemente de Legendre.

Otro resultado importante de Gauss, es la demostración de Teorema Fundamental del Algebra, del cual d'Alembert había dado una demostración, pero incompleta. Mediante este teorema se prueba la existencia de raíces complejas para cualquier polinomio con coeficientes en los complejos.

Su obra más famosa es *Disquisitiones Arithmeticae*, publicada en 1801, en donde Gauss sienta las bases de la teoría de números, como una de la disciplinas más sólidas y ricas de la matemática.

Gran parte de las *Disquisitiones*, están dedicadas al estudio de las formas cuadráticas binarias, iniciado por Legendre. Dicha teoría se expresa de manera más natural dentro de la moderna teoría de ideales de cuerpos cuadráticos, descubierta por Dedekind.

Estos cuerpos cuadráticos son de la forma

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b, \in \mathbb{Q}\}$$

Si I_d es el anillo de enteros algebráicos de $\mathbb{Q}(\sqrt{d})$, entonces Gauss fue el primero en determinar para cuáles d negativos, I_d es un dominio de ideales principales. Esto ocurre sólo en los casos

$$d = \text{-1, -2, -3, -7, -11, -19, -43, -67 y -163.}$$

Esta conjetura fue comprobada en 1975 por A.Baker y H. Stark .

Además Gauss conjeturó que existen infinitos $d > 0$ para los cuales I_d es un dominio de ideales principales. Esto no se ha podido demostrar hasta el presente.

En 1807 Gauss fue designado Director del Observatorio de Götingen, debido al éxito de sus investigaciones en astronomía, actividad ésta que compartió con la matemática durante toda su vida. En 1801 mediante unos cálculos asombrosos permitió redescubrir el planetoide Ceres, que había desaparecido de la vista de los astrónomos.

En Götingen pasó los últimos 50 años de su vida, trabajando como profesor de matemáticas e investigador, hasta su muerte en 1855. La obra de Gauss generó toda una nueva corriente de pensamiento dentro de la teoría de números, que nos conduce a la teoría de números algebráicos. Los herederos de la tradición de Gauss han sido Dirichlet, Dedekind, Kummer y Minkowsky , matemáticos éstos del siglo pasado y comienzos del actual, que generalizaron muchos de sus resultados.

La teoría de números ha tenido un desarrollo muy vigoroso a partir de entonces, con la introducción de nuevas técnicas como las teorías de ideales, formas cuadráticas, formas modulares, ... etc y ha permitido resolver muchos problemas de teoría de números elemental, que eran intratables con los métodos clásicos.

Capítulo

1

Los Números Enteros

1.1 Introducción

En este capítulo nos dedicaremos al estudio de los números enteros los cuales son el punto de partida de toda la teoría de números. Estudiaremos una serie de propiedades básicas de este conjunto, que son fundamentales para el posterior desarrollo de esta materia, como lo son el algoritmo de la división y el teorema de la factorización única.

Advertimos al lector sobre la necesidad de estudiar cuidadosamente el material expuesto en todas estas secciones de este capítulo, antes de pasar a los siguientes.

El enfoque usado en estas notas consiste en exponer inicialmente las propiedades básicas de los enteros, y a partir de éstas, ir deduciendo propiedades más avanzadas, como proposiciones, teoremas,..etc. En ningún momento nos planteamos dar un tratamiento formal y riguroso del tema de los números enteros, cosa que esta fuera del alcance de este curso. Para un estudio completo acerca de la construcción de los enteros a partir de los naturales, ver [1].

1.2 Definiciones Básicas

Supondremos que el lector está familiarizado con la notación de conjunto y además maneja los conceptos de pertenencia, inclusión, unión e intersección.

Definición 1.2.1 *Sean A y B dos conjuntos, una* **función de A en** *B, es una ley que asocia a cada elemento a de A, un único elemento b de B.*

Usamos la letra f para indicar la función, o bien el símbolo $f : A \longrightarrow B$. El elemento b se llama la **imagen** de a bajo la función f, y será denotada por $f(a)$.

Definición 1.2.2 *Sea $f : A \longrightarrow B$ una función y E un subconjunto de A, entonces la* **Imagen de E** *bajo f es el conjunto*

$$f(E) = \{b \in B \mid b = f(c), \text{ para algún } c \text{ en } E\}.$$

Es claro que $f(E)$ es un subconjunto de B.

Definición 1.2.3 *Sea $f : A \longrightarrow B$ una función y G es un subconjunto de B, la* **imagen inversa de G** *bajo f es el conjunto*

$$f^{-1}(G) = \{d \in A \mid f(d) \in G\}.$$

Definición 1.2.4 *Una función $f : A \longrightarrow B$ se dice* **Inyectiva** *si para todo b en B, $f^{-1}(\{b\})$ posee a lo sumo un elemento.*

Observación: Otra forma de definir la inyectividad de una función es la siguiente: Si cada vez que tengamos un par de elementos a y b en A, entonces si estos elementos son diferentes, sus imágenes deben ser diferentes.

Ejemplo: La función $F : \mathbb{N} :\longrightarrow \mathbb{N}$, donde $\mathbb{N}$ denota al conjunto de los números naturales, dada por $F(n) = 2n$, es inyectiva. ¿Podría el lector dar una demostración de este hecho?

Definición 1.2.5 *Sea $f : A \longrightarrow B$ una función. Diremos que f es* **Sobreyectiva** *si $f(A) = B$.*

Observación: El conjunto imagen de A, se llama también el **rango de la función**. Luego f es sobreyectiva si su rango es igual al conjunto de llegada.

Ejemplo: La función del ejemplo anterior no es sobreyectiva ¿Porqué?

Ejemplo: Sea $g : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $g(n) = n + 1$. Entonces esta función tampoco es sobreyectiva. Sin embargo si denotamos por $\mathbb{Z}$ al conjunto de los enteros y $G : \mathbb{Z} \longrightarrow \mathbb{Z}$, mediante $G(z) = z + 1$, entonces G si es una función sobreyectiva.

Definición 1.2.6 *Una función $f : A \longrightarrow B$ se dice* **biyectiva** *si f es inyectiva y sobreyectiva.*

Definición 1.2.7 *Sea A un conjunto cualquiera, una* **relación en A**, *es un subconjunto R del producto cartesiano $A \times A$.*

Si el par (a, b) está en R, diremos que a **está relacionado con** b, y lo denotamos por $a \sim b$, ó aRb.

Definición 1.2.8 *Una relación R sobre A, se dice que es de* **equivalencia**, *si satisface las tres condiciones*

1. *Reflexiva*
   $a \sim a$ para todo a en A.

2. *Simétrica*
   $a \sim b$ implica $b \sim a$, para todos a y b en A.

3. *Transitiva*
   Si $a \sim b$ y $b \sim c$, entonces $a \sim c$, para todos a, b y c en A.

Para cada a en A, el conjunto

$$[a] = \{b \in A \mid b \sim a\}$$

se llama **la clase de equivalencia de a**.

Definición 1.2.9 *Una* **operación binaria** *sobre un conjunto A, es una función $g : A \times A \longrightarrow A$.*

La imagen del elemento (a, b) bajo la función g se denota por $a * b$.

Ejemplos de operaciones son la suma y producto de números enteros. También se pueden definir operaciones en forma arbitraria. Por ejemplo, si $\mathbb{N}$ es el conjunto de números naturales, podemos construir la operación

$$* : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(a, b) \longrightarrow a * b = ab + 1.$$

1.3 Propiedades de los Enteros

Nosotros supondremos que el lector está familiarizado con el sistema de los números enteros $\ldots -2, -1, 0, 1, 2, 3, \ldots$, el cual denotaremos por $\mathbb{Z}$, así como también, con las propiedades básicas de adición y multiplicación. Podemos dar algunas de estas propiedades como axiomas y deducir otras, a partir de las primeras, como teoremas.

I) **Axiomas de Suma**

Existe una operación binaria en $\mathbb{Z}$, llamada la **suma de enteros**, la cual será denotada por $+$ y satisface :

1. **Cerrada**
   Para a y b números enteros, $a + b$ es un número entero

2. **Conmutativa**
   $a + b = b + a$, para todos a y b enteros .

3. **Asociativa**
   $(a + b) + c = a + (b + c)$, para todos a, b y c enteros.

4. **Elemento neutro**
   Existe un elemento en $\mathbb{Z}$ llamado el cero, el cual se denota por 0, y satisface:
   $$0 + a = a + 0 = a$$
   para todo a entero.

5. **Elemento opuesto**
   Para todo a en $\mathbb{Z}$ existe un elemento, llamado el opuesto de a, el cual denotamos por $-a$, y que satisface:
   $$a + (-a) = -a + a = 0$$

II) **Axiomas de Multiplicación**

Existe una operación binaria en $\mathbb{Z}$, llamada **producto de números enteros**, la cual se denota por $\cdot$, y satisface:

1. **Cerrada**
   Para a y b números enteros, $a \cdot b$ es un número entero

2. **Asociativa**
   Para a, b y c enteros

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. **Conmutativa**
   Para a y b enteros

$$a \cdot b = b \cdot a$$

4. **Elemento neutro**
   Existe un entero, llamado el uno y denotado por 1, tal que para todo entero a se tiene

$$1 \cdot a = a \cdot 1 = a$$

III) **Axioma de distributividad**
Para a, b y c enteros se cumple que

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Antes de pasar a ver otros axiomas de los números enteros, como son los axiomas de orden, necesitamos la siguiente definición.

Definición 1.3.1 *Una* **relación de orden** *en un conjunto A, es una relación R sobre A, con las siguientes propiedades:*

1. *Propiedad simétrica*
   Para todo a en A, se verifica aRa.

2. *Propiedad Transitiva*
   Para a, b y c en A se verifica: Si aRb y bRc, entonces aRc

3. *Propiedad antisimétrica*
   Si aRb y bRa entonces $a = b$.

Ejemplo: La relación "Menor o igual que", en el conjunto de los enteros, es ciertamente, una relación de orden. Esto puede ser verificado sin ninguna dificultad por el lector.

A continuación daremos una forma, quizás un poco rigurosa, de introducir esta relación, usando la suma de enteros y la existencia de un conjunto P. (Conjunto de enteros positivos).

IV) **Axiomas de Orden**

Existe un conjunto de enteros, llamados **enteros positivos**, el cual denotaremos por P, y que satisface:

1. Para todos a y b en P, $a+b$ y $a.b$ están en P.
2. 1 está en P.
3. **Ley de tricotomía**
   Para todo entero a se tiene una y sólo una de las siguientes:
   i) a está en P, ii) $-a$ está en P, iii) $a=0$.

Usando los axiomas de orden, se define la siguiente relación en el conjunto de los enteros:

Definición 1.3.2 *Sean a y b dos enteros, diremos que a* **es menor o igual que** *b, y lo denotamos por $a \leq b$, si y sólo si $b-a$ es positivo o cero.*

Definición 1.3.3 *Sean a y b dos enteros, diremos que a* **es menor que** *b, y lo denotamos por $a < b$ si y sólo si $a \leq b$ y $a \neq b$.*

También diremos que: a **es mayor o igual a** b, y lo denotamos por $a \geq b$ si b es menor o igual que a.

Igualmente, diremos que a es **mayor que** b, y se denota por $a > b$, si b es menor que a.

Observación: El conjunto P de enteros positivos es igual al conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, \ldots\}$, como veremos a continuación:

Notemos en primer lugar que 1 está en P (Axioma 2 de orden). Por la primera parte del axioma 1, se sigue que $2 = 1 + 1$, también está en P. De igual manera $3 = 2 + 1$, está en P, ... y así sucesivamente. De esta forma se concluye que el conjunto de los números naturales está en P. ¿Habrán otros elementos en P además de estos? La respuesta a esta pregunta, la podremos obtener como una consecuencia del teorema del mínimo elemento.

1.4 Axioma del Elemento Mínimo

Los axiomas estudiados hasta ahora no son suficientes para caracterizar el conjunto de los números enteros, en el sentido de determinar, sin ningún tipo de duda, todas y cada una de sus propiedades. A manera de ejemplo, la propiedad de infinitud de los enteros, no se puede derivar de ninguno de los axiomas o propiedades antes vistas. De aquí se concluye que es necesario incluir más axiomas, si se quiere tener un sistema completo, suficientemente bueno como para deducir, esta y otras propiedades que caracterizan a los enteros.

Definición 1.4.1 *Sea A un conjunto no vacío de $\mathbb{Z}$, entonces diremos que un entero a es una* **cota superior** *para A, si se cumple:*

$$n \leq a, \text{ para todo } n \text{ en } A \ .$$

Definición 1.4.2 *Diremos que un conjunto A está* **acotado superiormente***, si A posee una cota superior.*

Definición 1.4.3 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un elemento a del conjunto A se dice* **elemento maximal** *, si $n \leq a$ para todo n en A.*

Observación: La diferencia entre las definiciones 1.4.1 y 1.4.3 radica en lo siguiente: Un conjunto A de enteros puede tener una cota superior a, pero, posiblemente a no es un elemento del conjunto A, por tanto a no es un elemento maximal.

Definición 1.4.4 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un entero b se llama* **cota inferior** *para el conjunto A, si se cumple:*

$$b \leq x, \text{ para todo } x \text{ en } A$$

Definición 1.4.5 *Sea A un conjunto no vacío de $\mathbb{Z}$. Un elemento a de A se llama* **elemento minimal***(o elemento mínimo), si satisface:*

$$a \leq x, \text{ para todo } x \text{ en } A \ .$$

La misma observación que hicimos para el elemento maximal, se aplica al elemento minimal.

Axioma del mínimo elemento

Todo conjunto no vacío de números enteros positivos, posee un elemento minimal.

El axioma del mínimo elemento, es equivalente a otro axioma, llamado Principio de Inducción, el cual damos a continuación:

Principio de Inducción

Sea $P(n)$ una proposición que depende de un entero positivo n, y supongamos que:

1. $P(1)$ es cierta.
2. Si $P(k)$ es cierta, para un entero k, entonces $P(k+1)$ también es cierta.

Luego $P(n)$ es cierta para todo entero positivo n.

A partir del principio de inducción es posible probar una gran cantidad de fórmulas o identidades, que involucran un número positivo n.

Ejemplo: Probar la fórmula:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \tag{1.1}$$

Demostración:

A fin de utilizar el principio de inducción, haremos una proposición que depende de n, y la llamaremos $P(n)$. Luego probaremos que esta proposición satisface las condiciones 1) y 2) del principio, con lo cual se estará verificando para todo n. Por lo tanto hacemos:

$$\text{P(n)} = \text{“la fórmula (1.1) vale para todo } n\text{”}.$$

Notemos en primer lugar, que $P(1)$ se reduce a afirmar lo siguiente:

$$1 = \frac{1(1+1)}{2}$$

lo cual es evidentemente cierto.

Sea ahora, k un entero y supóngase que $P(k)$ es cierto, esto es:

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}.$$

Partiendo de esta ecuación, y sumando $k + 1$ a ambos lados, se tiene

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

Luego podemos sumar los dos términos en el lado derecho de la ecuación para obtener:

$$1 + 2 + 3 + \ldots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

Vemos entonces que esta última fórmula es igual a (1.1), con $n = k + 1$. Por lo tanto $P(k+1)$ es cierto, si se asume que $P(k)$ es cierto. Esto, unido a la veracidad de P(1), nos permite afirmar la validez de $P(n)$ para todo n.

♠

Ejemplo: Consideremos el **triángulo de Pascal:**

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & \ldots & & & &
\end{array}
$$

donde todos los elementos situados sobre los lados oblicuos son iguales a uno, y cada elemento interior es igual a la suma de los dos elementos adyacentes sobre la fila anterior.

Podemos denotar por $C(n, r)$ al elemento del triángulo de Pascal situado en la fila n y en la posición r (dentro de esta fila).

Luego se tendrá

$$C(0,0) = 1$$

$$C(1,0) = 1, \quad C(1,1) = 1$$

$$C(2,0) = 1, \quad C(2,1) = 2, \quad C(2,2) = 1$$

$$\ldots$$

y así sucesivamente.

En general se tiene la fórmula

$$C(n, r) = C(n-1, r-1) + C(n-1, r)$$

Este tipo de fórmula, en donde un elemento se define en función de los anteriores se llama **fórmula de recurrencia**. La posibilidad de definir elementos enteros mediante esta técnica de la recurrencia se debe al principio de inducción, ver [1].

Existe otra forma de expresar los coeficientes del triángulo de Pascal, explícitamente en función de n, la cual probaremos usando inducción. Más precisamente:

Proposición 1.4.1 *Si n es un entero positivo, entonces se tiene*

$$C(n,r) = \frac{n!}{(n-r)!\ r!} \qquad 0 \leq r \leq n. \tag{1.2}$$

Demostración:

Denotaremos por $P(n)$ la proposición (1.2), y probaremos que $P(n)$ es cierta para todo n, usando el principio de inducción.

El primer paso de la inducción corresponde a $n = 0$, lo cual nos da:

$$1 = C(0,0) = \frac{0!}{(0-0)!\ 0!}$$

siendo esto cierto, se tiene que $P(0)$ es cierto.

Sea n un entero positivo cualquiera, y supongamos que la relación (1.2) sea cierta. Luego debemos probar $P(n+1)$:

$$C(n+1,r) = \frac{(n+1)!}{(n+1-r)!\ r!} \qquad 0 \leq r \leq n+1$$

Sea r entero positivo, $0 < r < n+1$. Luego usando la fórmula de recurrencia para $C(n+1,r)$ se obtiene:

$$\begin{aligned} C(n+1,r) &= C(n,r) + C(n,r-1) \\ &= \frac{n!}{(n-r)!r!} + \frac{n!}{(n-r+1)!\ (r-1)!} \\ &= \frac{(r+1)!}{(n+1-r)!\ r!} \end{aligned}$$

Si $r = 0$, se tiene:

$$C(n+1,0) = 1 = \frac{(n+1)!}{(n+1-0)!\ 0!}$$

Si $r = n+1$ se tiene:

$$C(n+1,n+1) = 1 = \frac{(n+1)!}{((n+1)-(n+1))!\ (n+1)!}$$

Por lo tanto, hemos demostrado la veracidad de $P(n+1)$, a partir de la veracidad de $P(n)$. Luego la fórmula (1.2) es cierta para todo n. ♠

Observación: Los números $C(n,r)$ son los coeficientes de la expansión del binomio $(x+y)^n$ y por ello se les llama **coeficientes binomiales**

Ejercicios

1) (Binomio de Newton) Sean x e y números reales cualesquiera y sea n un entero positivo. Probar

$$(x+y)^n = \sum_{r=1}^{n} \left(\begin{array}{c} n \\ r \end{array} \right) x^{n-r} y^r$$

2) La **sucesión de Fibonacci**. La sucesión a_n definida por recurrencia $a_0 = 0$, $a_1 = 1 \ldots, a_{n+1} = a_n + a_{n-1}$, se denomina sucesión de Fibonacci. Demostrar, usando inducción sobre n, que el término general de esta sucesión viene dado por:

$$a_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

3) **El Número de Oro:**

El número $\varphi = (\frac{1+\sqrt{5}}{2})$ que aparece en la sucesión de Fibonacci, se llama el Número de Oro y posee propiedades muy interesantes. Este se obtiene como el cociente de los lados del rectángulo de lados a y b, tal que es proporcional al rectángulo de lados b, $a+b$. Esto es

$$\frac{b}{a} = \frac{a+b}{b}$$

Probar que el radio $\dfrac{b}{a}$ es igual a φ.

4) Si a_n es el término enésimo de la sucesión de Fibonacci, probar

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \varphi$$

5) Usando el principio de inducción, probar las fórmulas

1. $1 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
2. $1 + 3 + 5 + 7 + \ldots + 2n - 1 = n^2$
3. $1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$

6) Probar

$$\left(\begin{array}{c} n \\ 0 \end{array} \right) + \left(\begin{array}{c} n \\ 1 \end{array} \right) + \cdots + \left(\begin{array}{c} n \\ n \end{array} \right) = 2^n$$

7) Probar

$$\left(\begin{array}{c} n \\ 0 \end{array} \right)^2 + \left(\begin{array}{c} n \\ 1 \end{array} \right)^2 + \cdots + \left(\begin{array}{c} n \\ n \end{array} \right)^2 = \left(\begin{array}{c} 2n \\ n \end{array} \right)$$

8) Probar que no existe un número entero x con la propiedad:

$$0 < x < 1.$$

Ayuda: Suponiendo que tal x exista, consideremos el conjunto de enteros positivos $\{x, x^2, \ldots\}$, el cual es distinto del vacío y no tiene elemento minimal. Esto contradice el axioma del mínimo elemento.

9) Usando el ejercicio anterior, probar que si n es un número entero cualquiera, entonces no existe entero x con la propiedad:

$$n < x < n + 1$$

10) Probar el principio de inducción a partir del principio del mínimo elemento.

11) Probar que el conjunto de los números enteros no está acotado superiormente.

12) Probar que en $\mathbb{Z}$ valen las dos leyes de cancelación, es decir, para todo a, b y c en $\mathbb{Z}$, con $a \neq 0$, se tiene

$$ab = ac \Longrightarrow b = c$$

$$ba = ca \Longrightarrow b = c$$

13) Probar que si a y b son dos enteros diferentes de cero, entonces

$$ab = 0 \Longrightarrow a = 0 \quad \text{ó} \quad b = 0$$

14) Demuestre que no existe un entero $a \neq 0$, con la propiedad.

$$a + x = x,$$

para todo x entero.

15) Probar que toda función inyectiva $f : A \to A$, donde A es conjunto finito, es sobre.

16) Demuestre que cualquier elemento $a \in \mathbb{Z}$ satisface:
i) $a^m.a^n = a^{m+n}$
ii) $(a^n)^m = a^{nm}$,
para todos m y n enteros.

17) Una **partición** en un conjunto A, es una familia de subconjuntos $\{A_i\}$ de A, tales que.
i) $A_i \cap A_j \neq \emptyset$, para $i \neq j$.
ii) $\bigcup_{i \geq 1} A_i = A$.

Probar que toda relación de equivalencia en A determina una partición

18) Demuestre que cualquier conjunto de números enteros acotado superiormente posee un máximo.

19) Demuestre que si a es un entero positivo y b es un entero negativo, entonces ab es negativo.

20) Demuestre que si a y b son impares, entonces su producto es un número impar.

1.5 Máximo Común Divisor

En esta sección estudiaremos el famoso teorema de la división de los números enteros, y algunos resultados importantes que se derivan del mismo.

Teorema 1.5.1 *Sea a un entero positivo, y b un entero arbitrario. Entonces existen enteros p y q, únicos, tales que*

$$b = qa + r, \quad 0 \leq r < a.$$

El entero q se llama el **cociente** *y r se llama el* **resto**

Demostración:

Primero, probaremos que q y r existen, y posteriormente, probaremos que ellos son únicos.

En primer lugar, si $b = 0$, tomamos $q = r = 0$.

Sea b distinto de cero y consideremos el conjunto

$$D = \{b - ua \mid u \text{ es un entero}\}$$

Este conjunto contiene enteros positivos, pues si $b > 0$, basta tomar $u = 0$.

Si por el contrario $b < 0$, hacer $u = b$, con lo cual $b - ba > 0$, y $b - ba \in D$.

Por lo tanto el conjunto D^+, de elementos no negativos de D es diferente del vacío.

Por el axioma del mínimo elemento, este conjunto posee un elemento minimal r el cual pertenece a D^+.

Así pues, existe un entero q, tal que

$$r = b - qa,$$

o bien

$$b = qa + r, \quad 0 \leq r.$$

Si suponemos $r \geq a$, se tiene $r - a \geq 0$ y por lo tanto

$$b - qa - a = b - (q + 1)a \geq 0.$$

Esto es,

$$b - (q+1)a \in D^+$$

y

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

lo cual contradice la minimalidad del elemento r. Luego se debe tener $r < a$.

Unicidad:

Supongamos que existen otro par de enteros q' y r' los cuales satisfacen

$$b = q'a + r', \quad 0 \leq r' < a.$$

Probaremos que $q = q'$, para lo cual supondremos que $q' > q$. Luego se tiene

$$0 = b - b = (q'a + r') - (qa + r) = (q' - q)a - (r - r'),$$

de donde se obtiene

$$(q' - q)a = r - r' \geq a.$$

lo cual es una contradicción, pues $r - r' < a$. Similarmente si suponemos $q > q'$ llegamos a la misma contradicción. Por lo tanto, se debe tener $q = q'$, y de esto se sigue $r = r'$.

♠

Definición 1.5.1 *Sea a un entero positivo, y b un entero cualquiera. Diremos que a* **divide a** *b, y lo denotamos por $a \mid b$, si existe otro entero c tal que $b = ac$.*

También se dice que b **es divisible por** a, o bien a **es un divisor de** b. El concepto de divisibilidad es uno de los más importantes en toda la teoría de números. Uno de los problemas aún no resueltos, consiste en hallar todos los divisores de un número cualquiera dado.

Algunas de las propiedades básicas de la divisibilidad, se exponen en la siguiente proposición.

Proposición 1.5.1 *Sean a, b y c enteros distintos de cero. Entonces*

1. $1 \mid a$
2. $a \mid 0$
3. $a \mid a$
4. *Si* $a \mid b$ *y* $b \mid c$, *entonces* $a \mid c$.
5. *Si* $a \mid b$ *y* $a \mid c$, *entonces* $a \mid bx + cy$, *para todo par de enteros* x *e* y.

Demostración:

Ejercicio. ♠

Definición 1.5.2 *Sean* a *y* b *dos enteros positivos. Un entero positivo* d, *se dice* **Máximo Común Divisor** *entre* a *y* b, *si y sólo si satisface*

1. $d \mid a$ *y* $d \mid b$
2. *Si* c *es otro entero positivo con la condición :*

$$c \mid a \quad \text{y} \quad c \mid b, \quad \text{entonces} \quad c \mid d.$$

El entero positivo d, se denota por $d = (a, b)$. De acuerdo a la definición, se tiene que el Máximo Común Divisor d, es el mayor de los divisores comunes de a y b.

Ejemplo: Hallar el Máximo Común Divisor entre 12 y 18.

En primer lugar, buscamos por tanteo, todos los divisores comunes de ambos números

Divisores de 12 : 1, 2, 3, 4, 6 y 12.
Divisores de 18 : 1, 2, 3, 6, 9 y 18.

Es evidente que el mayor divisor común es 6, y por lo tanto concluimos

$$(12, 18) = 6.$$

Existe un método práctico para calcular el Máximo Común Divisor entre dos números, el cual está basado en el algoritmo de división. Este método, llamado **Método de Euclides para el M.C.D.** consiste en una serie de divisiones sucesivas y, el Máximo Común Divisor se obtiene como uno de los restos en el proceso de división. Además de dar una forma constructiva de calcular el M.C.D., permite al mismo tiempo dar una demostración de la existencia de éste.

Teorema 1.5.2 Método de Euclides
Dados dos enteros positivos a y b, el Máximo Común Divisor entre ellos, $d = (a, b)$, siempre existe.

Demostración:

Podemos suponer, sin pérdida de generalidad que $b > a > 0$. Luego por el teorema de división, existen enteros q_1 y r_1 tales que

$$b = q_1 a + r_1, \quad 0 \leq r_1 < a.$$

Si $r_1 = 0$, entonces $b = q_1 a$ y por lo tanto $(b, a) = a$, con lo cual queda demostrado el teorema.

Si $r \neq 0$, podemos aplicar de nuevo el teorema de la división, para obtener un par de enteros q_2, r_2 tales que

$$a = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

Continuando de esta manera, se obtiene una sucesión de enteros positivos decrecientes: $r_1 > r_2 > \ldots > 0$. Es evidente que esta sucesión es finita y por lo tanto existe n, tal que $r_n \neq 0$ y $r_{n+1} = 0$. Luego existen enteros $q_1, q_2, \ldots q_{n+1}, r_1, r_2, \ldots, r_n$ que cumplen las relaciones:

$$\begin{aligned} b &= aq_1 + r_1, \quad 0 < r_1 < b \\ a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} \end{aligned}$$

Afirmamos que $(a, b) = r_n$.

En primer lugar, notemos que de la última ecuación se tiene que r_n divide a r_{n-1} . Por lo tanto, $r_n \mid (r_{n-1}q_n + r_n)$, es decir r_n divide a r_{n-2}. Continuando de esta manera, llegamos finalmente, a que r_n divide a todos los demás r_i . En particular

$$r_n \mid r_1 \quad y \quad r_n \mid r_2, \quad \text{implica que} \quad r_n \mid r_1q_2 + r_2$$

luego $r_n \mid a$.

Igualmente, usando $r_n \mid a$ y $r_n \mid r_1$ se deduce $r_n \mid b$.

Finalmente, si c es un entero positivo que divide a a y a b, se tiene

$$c \mid b - aq_1,$$

o sea, $c \mid r_1$. Continuando de esta manera, se tiene que $c \mid r_i$ para todo i y por tanto $c \mid r_n$.

Con esto hemos demostrado las dos condiciones de la definición de Máximo Común Divisor para r_n y por lo tanto $(a, b) = r_n$.

♠

Ejemplo: Podemos calcular el Máximo Común Divisor entre 672 y 38, usando el método anterior, para lo cual haremos las divisiones correspondientes. Luego

$$672 = 17 \cdot 38 + 26$$

$$38 = 1 \cdot 26 + 12$$

$$26 = 2 \cdot 12 + 2$$
$$12 = 6 \cdot 2$$

El último resto diferente de cero es 2, luego $(672, 38) = 2$.

En la demostración del teorema anterior, obtuvimos las ecuaciones

$$\begin{aligned} r_1 &= b - aq_1 \\ r_2 &= a - r_1 q_2 \\ &\vdots \\ r_{n-1} &= r_{n-3} - r_{n-2} q_{n-1} \\ r_n &= r_{n-2} - r_{n-1} q_n \end{aligned}$$

Observamos que el Máximo Común Divisor entre a y b, dado por r_n viene expresado en función de r_{n-2} y r_{n-1}. Ahora bien, en la penúltima ecuación se puede reemplazar r_{n-1} en función de r_{n-2} y r_{n-3}. Continuando de esta forma, podemos ir sustituyendo los valores de r_i en función de los anteriores, hasta que tengamos r_n en función de a y b. Así pues hemos demostrado el siguiente resultado:

Teorema 1.5.3 *El Máximo Común Divisor entre dos enteros a y b, se expresa como combinación lineal de a y b. Es decir, existen enteros x e y tales que*

$$(a, b) = ax + by$$

Ejemplo: Podemos expresar el Máximo Común Divisor entre 672 y 38 como combinación lineal de ambos, para lo cual usamos las cuatro ecuaciones del ejemplo anterior.

$$\begin{aligned} 2 &= 26 - 2 \cdot 12 \\ 2 &= 26 - 2 \cdot (38 - 26) \\ 2 &= 3 \cdot 26 - 2 \cdot 38 \\ 2 &= 3 \cdot (672 - 17 \cdot 38) - 2 \cdot 38 \\ 2 &= 3 \cdot 672 - 53 \cdot 38 \end{aligned}$$

Una de las aplicaciones de mayor utilidad que ofrece el teorema de la división, es la representacion de cualquier número mediante combinación lineal de potencias de 10.

Teorema 1.5.4 *Si b es un entero positivo, entonces existen enteros únicos $r_0, r_1, \ldots, r_n$ tales que*

$$b = r_n 10^n + r_{n-1} 10^{n-1} + \ldots + r_1 10 + r_0$$

con $0 \leq r_i < 10$ para todo i.

Demostración:

Usaremos inducción sobre b. Si $b = 1$ es cierto. Supongamos el resultado cierto para todo entero menor que b, y probaremos la afirmación para b. Podemos dividir b entre 10 para obtener enteros únicos q y r_0 tales que

$$b = q \cdot 10 + r_0, \quad 0 \leq r_0 < 10$$

Como q es menor que b, aplicamos la hipótesis de inducción a q. Luego existen enteros únicos $r_1, r_2, \ldots, r_n$, con $0 \leq r_i < 10$, tales que

$$q = r_n 10^{n-1} + \ldots + r_2 10 + r_1$$

Por lo tanto

$$b = (r_1 + r_2 10 + \ldots + r_n 10^{n-1})10 + r_0$$

$$= r_n 10^n + \ldots + r_1 10 + r_0$$

Es claro que todos los r_i son únicos. Con esto termina la demostración.

♠

Definición 1.5.3 *Dos enteros positivos a y b, se dicen* **primos relativos** *si el Máximo Común Divisor entre ellos es uno.*

Ejemplo: Los enteros 20 y 9 son primos relativos, pues $(20, 9) = 1$. Nótese que 20 y 9 no son números primos.

El siguiente resultado, que caracteriza las parejas de enteros primos relativos, será de mucha utilidad en el futuro:

Teorema 1.5.5 *Dos enteros positivos a y b son primos relativos, si y sólo si existen enteros x e y tales que*

$$ax + by = 1$$

Demostración:

Es claro que existen enteros x e y, tal que

$$ax + by = 1$$

pues 1 es el Máximo Común Divisor entre a y b.

Por otro lado, si suponemos $ax + by = 1$, para algunos enteros x e y, podemos probar $(a, b) = 1$. En efecto, si c es un divisor de a y b, se tendrá que c divide a $ax + by$, o sea c divide a 1. Luego $c = 1$, y por lo tanto el Máximo Común Divisor entre a y b es 1.

♠

Definición 1.5.4 *Sean a y b dos enteros positivos, el* **mínimo común múltiplo** *entre a y b, es otro entero positivo c, el cual satisface:*

1. $a \mid c$ *y* $b \mid c$
2. *Si e es otro entero, tal que $a \mid e$ y $b \mid e$, se tiene $c \mid e$.*

De la definición anterior se sigue que c es el menor múltiplo común entre a y b.

Usaremos la notación :

$$[a, b] = \text{mínimo común múltiplo entre } a \text{ y } b.$$

Proposición 1.5.2 *Sean a, b, y c tres enteros positivos, tales que $(a, b) = 1$ y $a \mid bc$. Luego $a \mid c$.*

Demostración:

Por el teorema anterior, existen enteros x e y tales que

$$ax + by = 1$$

Multiplicando por c tenemos

$$cax + cby = c$$

Por hipótesis, sabemos que $a \mid bc$, luego $a \mid cby$. También se tiene $a \mid cax$, y por lo tanto concluimos

$$a \mid cax + cby$$

lo cual implica que $a \mid c$.

♠

Para finalizar esta sección, daremos una serie de propiedades fundamentales del Máximo Común Divisor:

Proposición 1.5.3 *Sean a, b y c enteros positivos. Entonces*

1. *Si m es otro entero tal que $m \mid a$ y $m \mid b$ se tiene*

$$\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{(a,b)}{m}$$

2. *Si n es cualquier entero*

$$(na, nb) = n(a, b)$$

3. *Si $(a, b) = d$, entonces*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

4. *Si x es cualquier entero, entonces*

$$(b, a + bx) = (a, b)$$

Demostración:

1) Sea $d = (a, b)$, y probaremos

$$\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{d}{m}$$

Notemos en primer lugar que d/m es un entero. En efecto se tiene $ax + by = d$, y por lo tanto

$$\frac{a}{m}x + \frac{b}{m}y = \frac{d}{m}$$

en el lado izquierdo de la ecuación tenemos un entero, luego d/m es entero.

Por otra parte, como d divide a a, se tiene que d/m divide a a/m. Igualmente se tendrá que d/m divide a b/m.

Finalmente, si c es otro entero que divide a a/m y b/m, se tendrá

$$\frac{a}{m} = cj \quad y \quad \frac{b}{m} = ck$$

para algunos enteros j y k.

Multiplicando ambas ecuaciones por m nos da

$$a = mcj \quad y \quad b = mck$$

de donde obtenemos

$$mc \mid a \quad y \quad mc \mid b$$

Usando la definición de Máximo Común Divisor para d, se tiene que d divide a mc, y por lo tanto d/m divide a c.

Así pues, hemos probado 1).

2) Usando 1) se tiene

$$(a, b) = \left(\frac{an}{n}, \frac{bn}{n}\right) = \frac{(an, bn)}{n}$$

luego

$$n(a, b) = (an, bn)$$

3) Usar 1) con $m = (a, b)$.

4) Observar que $(a, b) \mid a$ y $(a, b) \mid b$. Luego $(a, b) \mid ax + b$.
Si c es un entero que divide tanto a b como a $a + bx$, se tendrá

$$c \mid ((a + bx) - bx)$$

y en consecuencia $c \mid a$.

Luego c divide al máximo común divisor entre a y b, el cual es d. Así pues, hemos probado $(b, a + bx) = (a, b) = d$.

♠

Ejemplo:

$$(200, 300) = (2, 3)100 = 100.$$

Ejercicios

1) Usando el algoritmo de Euclides, hallar
a) (122,648)
b) (715,680)
c) (1581,206)
d) (3742, 843)
e) (120, 560)
f) (458, 1290).

2) Demuestre que si $(a, b) = 1$, entonces:

$$(a - b, a + b) = 1, \quad \text{ó} \quad 2.$$

3) Demuestre que si $ax + by = m$, entonces $(a, b) \mid m$.

4) Demuestre que si $(b, c) = 1$, entonces para todo entero positivo a, se tiene $(a, bc) = (a, b)(a, c)$.

5) El Máximo Común Divisor para tres números enteros positivos a, b y c, denotado por (a, b, c) se define como el entero positivo d que satisface:

1. $d \mid a, \quad d \mid b, \quad y \quad d \mid c$

2. Si f es otro entero tal que $f \mid a$, $f \mid b$ y $f \mid c$ entonces $f \mid d$.

Probar que $(a, b, c) = ((a, b), c) = (a, (b, c))$.

6) Hallar el Máximo Común Divisor de
   a) (23,12,18)
   b) (90, 80, 56)
   c) (65, 20, 190).

7) Hallar una solución en números enteros de la ecuación

$$21x + 25y = 1$$

8) Probar que el mínimo común múltiplo entre dos enteros a y b siempre existe.

9) Demostrar la fórmula

$$[a, b] = \frac{ab}{(a, b)}$$

10) Usando la fórmula anterior, calcular
   a) [12,28]
   b) [120,50]
   c) [34,62]
   d) [88, 340].

1.6 Teorema de Factorización Unica

Definición 1.6.1 *Un entero positivo p, distinto de 1, se dice que es* **primo** *si los únicos divisores de p son 1 y p.*

Ejemplo: Los números 2, 3, 19 son primos.

Los números enteros positivos que no son primos, se les llama **compuestos**, como por ejemplo 6. Es decir, todo número compuesto es de la forma

$$m = m_1 m_2,$$

donde $1 < m_1 < m$ y $1 < m_2 < m$.

Los números primos y su distribución dentro de los números enteros, han sido estudiados desde la antigüedad. Ellos han ejercido una atracción fascinante sobre los matemáticos, debido a la forma tan irregular como aparecen en la sucesión de los enteros. Muchos matemáticos han tratado en vano de hallar una fórmula que genere exclusivamente números primos. Así por ejemplo, Pierre Fermat conjeturó que todo número de la forma

$$s(n) = 2^{2^n} + 1$$

era primo. Esto lo comprobó para n= 1,2,3 y 4. Sin embargo en 1732 Leonhard Euler demostró que $s(5)$ no era primo.

Existe una gran cantidad de problemas, aún no resueltos, sobre los números primos. Algunos de ellos serán tratados en las próximas secciones.

El método más elemental para hallar la sucesión de los primos, es el llamado **Criba de Eratóstenes**. Este consiste en colocar los números enteros positivos en orden creciente, formando diez columnas de la siguiente forma

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

.....

Entonces comenzamos por eliminar de la lista todos los números pares, luego los múltiplos de tres, luego los de cinco, ... y así sucesivamente, hasta agotar todos los números compuestos. Es evidente que los restantes números en la lista serán todos los números primos.

Teorema 1.6.1 *Todo número entero positivo, mayor que uno, puede ser factorizado como un producto de números primos.*

Demostración:

Sea m el número en cuestión. Usaremos inducción sobre m, para probar la proposición "m puede ser factorizado como un producto de primos".

En primer lugar, la proposición es cierta para $m = 2$, pues 2 mismo es un número primo. Supóngase la veracidad de la proposición, para todo número menor que un cierto k, es decir, todo número menor que k y mayor o igual a dos, puede ser factorizado como producto de primos.

Consideremos ahora k. Si k es primo, entonces no hay nada que probar y el resultado será cierto para k. Si por el contrario, k resulta ser compuesto, entonces tenemos

$$k = m_1 m_2$$

donde $2 \leq m_1 < k$ y $2 \leq m_2 < k$.

Podemos entonces aplicar la hipótesis de inducción, tanto a m_1 como a m_2, es decir cada uno de ellos se factoriza como un producto de primos. Luego

$$m_1 = p_1 p_2 \dots p_s$$

$$m_2 = q_1 q_2 \dots q_t$$

donde los p_i, q_j son números primos.

Por lo tanto tenemos

$$k = m_1 m_2 = p_1 p_2 \dots p_s q_1 q_2 \dots q_t$$

esto es, un producto de primos.

♠

Observación: Es posible tener algunos primos repetidos en la factorización de un número compuesto. Por ejemplo $24 = 2.2.2.3$. En todo caso, podemos agrupar aquellos primos iguales usando potenciación. Esto es todo entero positivo n puede ser escrito de la forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \tag{1.3}$$

donde los p_i son todos primos diferentes y los α_i son mayores o iguales a uno.

La siguiente proposición es fundamental para la demostración del teorema de factorización única.

Proposición 1.6.1 *Sean $p, p_1, p_2, , \ldots p_n$ números primos, tales que $p \mid p_1.p_2 \ldots p_n$. Entonces $p = p_i$ para algún i.*

Demostración:

Usaremos inducción sobre n.

Para $n = 1$, el resultado es cierto. Supongamos que p es distinto de p_1, entonces tenemos

$$(p, p_1) = 1 \quad y \quad p \mid p_1(p_2 p_3 \ldots p_n)$$

Luego por la proposición 2 se obtiene

$$p \mid p_2.p_3 \ldots p_n$$

Usando la hipótesis de inducción, se concluye que $p = p_i$ para algún i.

♠

Teorema 1.6.2 *Todo número entero positivo n, tiene una factorización única de la forma*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$$

Demostración:

Supongamos que n tiene dos factorizaciones distintas

$$n = p_1^{\alpha_1} \ldots p_s^{\alpha_s} = q_1^{\beta_1} \ldots q_t^{\beta_t} \tag{1.4}$$

Probaremos en primer lugar que $s = t$ y posteriormente probaremos que para todo i, con $1 \leq i \leq s$, se tiene

$$p_i = q_j, \quad \text{para algún} \quad j \ \text{ y } \quad \alpha_i = \beta_j.$$

Usaremos inducción sobre n. Si $n = 1$, entonces la tesis del teorema se cumple.

Supongamos que el teorema es cierto para todo entero positivo k, con $k < n$ y probemos el resultado para n.

Sea entonces n como en (1.4). Notemos que p_1 divide al producto de primos $q_1^{\beta_1} \dots q_t^{\beta_t}$, luego por el lema anterior p_1 debe ser igual a alguno de ellos, digamos q_i. Podemos entonces cancelar p_1 en ambos lados de (1.4), con lo cual tendremos que n/p_1 posee dos factorizaciones. Si se aplica entonces la hipótesis de inducción se obtiene el resultado.

♠

Uno de los primeros resultados acerca de los números primos, y que aparece demostrado en *Los Elementos* de Euclides, es el siguiente.

Teorema 1.6.3 *Existen infinitos números primos.*

Demostración:

Supóngase que hay solamente un número finito de primos, digamos $p_1, p_2, \dots, p_n$. Entonces el número

$$x = p_1 p_2 \dots p_n + 1$$

puede ser factorizado como producto de primos.

Sin embargo, ningún primo p_i, de los antes mencionados, puede estar entre los factores de x, pues p_i no divide a x; ¿Por qué?

♠

Ejercicios

1) Hallar la descomposición en factores primos de
   a) 165
   b) 670
   c) 124

d) 1567
e) 444.

2) Por medio de la Criba de Eratóstenes, hallar todos los primos menores que 200.

3) Probar que si n no es primo, entonces n tiene un divisor primo, el cual es menor o igual a $\sqrt{n}$.

4) Usando el resultado anterior, implemente un algoritmo de computación para determinar cuándo un número es primo.

5) Determine cuáles de los siguientes números son primos:
a) 941
b) 1009
c) 1123
d) 1111
e) 671
f) 821.

6) Algunos primos son de la forma $4k + 1$, como por ejemplo, 5, 17, 101, ... etc. Probar que hay infinitud de ellos.

7) Demostrar que $2^{524} - 1$ no es primo.

8) Sea

$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

y

$$b = p_1^{\beta_1} \dots p_n^{\beta_n},$$

entonces probar

$$(a, b) = p_1^{\delta_1} \dots p_n^{\delta_n}$$

donde $\delta_i = min\{\alpha_i, \beta_i\}$.

$$[a, b] = p_1^{\gamma_i} \dots p_n^{\gamma_n}$$

donde $\gamma_i = max\{\alpha_i, \beta_i\}$

9) Use el ejercicio anterior para hallar
a) $(240, 45)$
b) $[240, 45]$.
c) $[1650, 7800]$

d) $[235, 7655]$

10) Probar que $\sqrt{5}$ es un número irracional.

Capítulo

2

Congruencias

2.1 Definiciones básicas

Definición 2.1.1 *Sea m un entero fijo, diremos que dos enteros a y b son* **congruentes módulo** *m , y usamos la notación*

$$a \equiv b \, mod \, m$$

si y sólo si m divide a $a - b$

Ejemplo: $25 \equiv 4 \, mod \, 7$, pues 7 divide a 25 - 4 = 21.

Observación: Podemos decir que a es congruente a b módulo m si existe un entero k, tal que $a = b + km$.

También se puede definir congruencia, usando el concepto de pertenencia. Más precisamente a es congruente a b módulo m si y sólo si a está en la sucesión de enteros

$$\ldots, b - m, b, b + m, b + 2m, \ldots$$

Cuando a y b no son congruentes módulo m, diremos que son **incongruentes** y lo denotaremos por $a \not\equiv b \, mod \, m$.

La notación de congruencias fue introducida por Gauss en su libro *Disquisitions Arithmeticae*, en 1799. Gauss desarrolló gran parte de la teoría de congruencias, planteó muchos problemas interesantes sobre este tema y resolvió algunos de ellos. Uno de los más importantes fue la resolución de la ecuación cuadrática de congruencias.

La noción de congruencia se utiliza a diario para medir el tiempo. Por ejemplo las horas del día se cuentan módulo 24, los días de la semana se cuentan módulo 7 , etc...

En lo sucesivo, m será un entero positivo fijo.

Teorema 2.1.1 *Sean a, b y c enteros cualesquiera. Entonces se tiene*

1. $a \equiv a \, mod \, m$
2. *Si* $a \equiv b \, mod \, m$, *entonces* $b \equiv a \, mod \, m$.
3. *Si* $a \equiv b \, mod \, m$, *y* $b \equiv c \, mod \, m$, *entonces* $a \equiv c \, mod \, m$.

Demostración:

1) Notemos que m divide a $a - a = 0$, luego $a \equiv a \ mod \ m$.

2) Se tiene que m divide a $b - a$, por hipótesis, luego $m| - (b - a)$, y por lo tanto $m \mid a - b$.

3) Por hipótesis se tiene $m \mid b-a$ y $m \mid c-b$. Luego $m \mid (b-a)+(c-b)$, esto es $m \mid c - a$. Por lo tanto $a \equiv c \ mod \ m$.

♠

Observación: Las tres propiedades anteriores para la relación de congruencia, nos indican que ésta es una relación de equivalencia (Ver Capítulo 1). Como resultado de esto, se obtiene una partición en el conjunto de los enteros en clases de equivalencia disjuntas, las cuales llamaremos **clases de congruencia módulo** m.

Definición 2.1.2 *Sea a un entero cualquiera, entonces la clase de congruencia de a módulo m, es el conjunto*

$$[a] = \{x \ entero \mid x \equiv a \ mod \ m\}$$

El entero a en la definición anterior se llama el **representante de la clase** y puede ser elegido arbitrariamente de entre los elementos de la clase: esto es, si $b \equiv a \ mod \ m$ entonces $[a] = [b]$.

Ejemplo: Si se considera la relación de congruencia módulo 7, se tendrá entonces:

$$[0] = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$$

$$[1] = \{\ldots, -13, -6, 1, 8, 15, \ldots\}$$

$$[2] = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$$

$$\vdots$$

$$[6] = \{\ldots, -8, -1, 6, 13, 20, \ldots\}$$

Ejemplo:. *Las horas.*

Para contar el tiempo en un mismo día, usamos las horas. Un día tiene 24 horas exactas y para contar las horas comenzamos por la hora 1, que es cuando comienza el día. Técnicamente, el día comienza en un instante 0 y contando 12 horas a partir de ese instante, el sol se hallará en la posición más alta del firmamento. Así pues, la primera hora comienza en el instante 0, la segunda después de una hora, ... y así sucesivamente hasta la hora 24. Al finalizar la hora 24 comienza un nuevo día y aquí reiniciamos el conteo de las horas. Es decir contamos las horas módulo 24.

Por ejemplo, si en este momento son las 8 p.m. ¿Qué hora será dentro de 200 horas?

Solución:

En primer lugar, si x es la hora buscada, debemos tener

$$x \equiv 20 + 200 \ mod \ 24$$

luego podemos reducir el lado derecho de esta ecuación "módulo 24". Así se obtiene

$$x \equiv 4 \ mod \ 24$$

Luego la hora x será las 4 a.m.

Ejercicios

1) Probar que las tres definiciones de la noción de congruencia, dadas al comienzo, son equivalentes.

2) Si hoy es jueves, entonces ¿que día de la semana será ...
a) dentro de 20 días?,
b) dentro de 100 días ?

3) Indicar cuáles de las siguientes afirmaciones son correctas y cuáles son falsas

1. $18 \equiv 1 \ mod \ 5$
2. $86 \equiv 1 \ mod \ 5$
3. $100 \equiv 10 \ mod \ 9$
4. $62 \not\equiv 2 \ mod \ 8$
5. $10^3 \equiv 1 \ mod \ 9$
6. $2a \equiv 6 \ mod \ 2$
7. $s^2 + s + 1 \equiv 1 \ mod \ 2$
8. $a(a+1)(a+2) \equiv 0 \ mod \ 3$

4) Probar que si $a \equiv b \ mod \ m$, entonces $a \equiv b \ mod \ k$, para todo k divisor de m. ¿Será cierto el recíproco de este resultado? Dar un contraejemplo.

5) Si hoy es jueves 27 de octubre de 1993, entonces ¿que día de la semana será el 27 de octubre de 1994? Use congruencias para hallar el resultado.

2.2 Propiedades de las Congruencias

A continuación damos una serie de propiedades de las congruencias, relacionadas con la suma y el producto de números enteros.

Teorema 2.2.1 *Si $a \equiv b \ mod \ m$, y c es un entero, se tiene*

1. $a + c \equiv b + c \ mod \ m$.
2. $ac \equiv bc \ mod \ m$

Demostración:

1) Si $a \equiv b \ mod \ m$, se tendrá entonces $m \mid b - a$. Luego $m \mid (a + c) - (b + c)$, y de aquí obtenemos

$$a + c \equiv b + c \ mod \ m$$

2) Se tiene $m \mid a - b$, y por lo tanto $m \mid (a - b)c$. Luego $m \mid ab - ac$, lo cual implica

$$ac \equiv bc \ mod \ m.$$

♠

Ejemplo: La ecuación de congruencia $1 \equiv 10 \ mod \ 9$, se puede multiplicar por 30, para obtener $30 \equiv 300 \ mod \ 9$.

Observación: El recíproco del teorema anterior no es cierto en general. Es decir de la congruencia $ca \equiv cb \ mod \ m$ no se puede inferir $a \equiv b \ mod \ m$. Por ejemplo $12 \equiv 6 \ mod \ 6$, pero $6 \not\equiv 3 \ mod \ 6$.

Seguidamente, daremos un par de propiedades mediante las cuales podemos multiplicar y sumar ecuaciones de congruencias, de la misma forma como se hace para las ecuaciones normales.

Teorema 2.2.2 *Sean a, b y c enteros con*

$$a \equiv b \ mod \ m \quad \text{y} \quad c \equiv d \ mod \ m.$$

Entonces se tiene

1. $a + c \equiv b + d \ mod \ m$

2. $ac \equiv bd \ mod \ m$

Demostración:

1) Si $a \equiv b \ mod \ m$, entonces existe un entero k tal que $a = b + km$. Igualmente de $c \equiv d \ mod \ m$, se obtiene un entero h, tal que $c = d + hm$. Luego

$$a + c = b + d + (h + k)m$$

y de aquí se sigue que:

$$a + c \equiv b + d \ mod \ m.$$

2) También tenemos

$$ac = (b + km)(d + hm) = bd + (bh + dk + hkm)m$$

y de esto se sigue que $ac \equiv bd \ mod \ m$. ♠

Teorema 2.2.3 *(***Congruencia de Polinomios***)*

Sea

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0,$$

un polinomio con coeficientes enteros. Entonces si $a \equiv b \ mod \ m$ *se tendrá:*

$$f(a) \equiv f(b) \ mod \ m.$$

Demostración:

Partiendo de la congruencia $a \equiv b \ mod \ m$, y aplicando el teorema anterior parte 2) tantas veces como se desee, deducimos

$$a^i \equiv b^i \ mod \ m \quad \text{para todo } \ 1 \leq i \leq n.$$

Multiplicando cada ecuación por su respectivo coeficiente nos da

$$c_i a^i \equiv c_i b^i \ mod\ m$$

Finalmente, podemos sumar todas estas ecuaciones, gracias al teorema 2.2.1 parte 1), para obtener el resultado deseado

$$c_n a^n + \ldots + c_1 a + c_0 \equiv c_n b^n + \ldots + c_1 b + c_0 \ mod\ m$$

luego, hemos probado $f(a) \equiv f(b)\ mod\ m$.

2.3 Cronología

En esta sección estudiaremos algunas aplicaciones de las congruencias en la cronología, como por ejemplo la determinación del día de la semana de una fecha determinada.

El Calendario Gregoriano

El origen de nuestro calendario actual se encuentra en el **Calendario Juliano**, llamado así por Julio César, quien participó activamente en el diseño de éste. En dicho calendario cada año constaba de 365 días y cada cuatro años había un año bisiesto de 366 días. El calendario de 12 meses comenzaba en el mes de Marzo y finalizaba en Febrero. El nombre y duración de los meses era el siguiente:

Nombre del mes	No. de días	Nombre en Latín
Marzo	30	Martius
Abril	30	Aprilis
Mayo	31	Maius
Junio	30	Junius
Quinto	31	Quintilis
Sexto	31	Sextilis
Septiembre	30	Septembris
Octubre	31	Octobris
Noviembre	30	Novembris
Diciembre	31	Decembris
Enero	31	Januaris
Febrero	28	Februarius

Durante el tiempo de César el mes quinto cambió de nombre por julio, en honor a este emperador. Más tarde, el mismo Julio César decidió que el año debería comenzar en enero. De esta manera quedó organizado el calendario sin sufrir ninguna modificación hasta la reforma del Papa **Gregorio XIII** en 1582.

Los años eran numerados de acuerdo al período de cada emperador, hasta el triunfo del cristianismo, cuando se comenzó a enumerarlos en forma diferente. A partir de entonces, el año 1 fue el nacimiento de Cristo y el día de Navidad el primer día de la Era Cristiana, luego los años se cuentan en sucesión creciente, partiendo desde este inicio. Esta reforma fue hecha en el 533 d.c. durante el período del Emperador Dionisio Exigus.

Una de las motivaciones que han tenido todos los pueblos en el momento de establecer un calendario, es la de ubicar correctamente las fiestas religiosas. Así observamos que en el Calendario Cristiano, el Domingo de Pascua determina las otras fechas movibles como la Ascensión y el Corpus Cristi. Durante el Concilio de Nicea en el 325 d.c. se acordó fijar esta fecha, como el primer domingo después de luna nueva que aparezca en el Equinoccio de Primavera (21 de Marzo) o después . Si la luna nueva aparece un domingo, entonces el Domingo de Pascua será el domingo siguiente.

Si bien el Calendario Juliano funcionó bien durante algunos siglos, la celebración de una Semana Santa a fines del siglo XVI, en donde el Domingo de Pascua correspondió al 11 de Marzo, hizo pensar a muchos que este calendario estaba lejos de ser perfecto. Veamos el por qué de semejante error y las rectificaciones que se le hicieron a el mismo, a fin de ajustarlo al tiempo sideral.

El **año astronómico**, una revolución completa de la tierra alrededor del sol, es de 365 días, 6 horas, 9 minutos y 9.5 segundos. Sin embargo el año visible o **año tropical**, período entre dos equinoccios de primavera, es más corto: 365 días, 5 horas, 48 minutos y 46.43 segundos. El Calendario Juliano suponía que el año tenía 365 días y un cuarto, lo cual excede en 11 minutos y 14 segundos al año tropical. Como consecuencia de esto, se comete un error de un día cada 128 años.

A fin de corregir este error, el Papa Gregorio XIII introdujo una reforma en el calendario, mediante la cual se eliminaron 10 días de la historia . Se decidió que el día siguiente al 4 de octubre de 1582, fuese el 15 de octubre. Además se redujeron los años bisiestos mediante la siguiente convención. Los años bisiestos seculares (divisibles por 100) serían sólo aquellos divisibles por 400. Así, por ejemplo 1800 y 1900 no son bisiestos, pero 2000 será bisiesto.

Esta reforma del Calendario Juliano se conoce con el nombre de **Calendario Gregoriano** y es el calendario que se ha venido usando hasta el presente.

Una vez hecha esta exposición de nuestro calendario, pasemos a calcular los días de la semana de algunas fechas históricas importantes. Nótese la importancia de las congruencias, en cuanto a su capacidad de simplificar los cálculos considerablemente.

Ejemplo: ¿Que día de la semana fue el 19 de abril de 1810?

Solución:

En primer lugar, calculamos el número de años bisiestos entre 1993 y 1810. Vemos que 1812 fue bisiesto y cien años más tarde 1912 ocurrieron 25 años bisiestos (descontamos a 1900 que no fue bisiesto). Entre 1912 y 1993 hay 20 años bisiestos, lo cual da un total de 45 años bisiestos desde 1810 hasta 1993. Luego calculamos el desfase entre ambos años relativo a los días de la semana. En otras palabras nos interesa la diferencia x en días desde 1810 hasta 1993 módulo 7.

Usando congruencias tenemos:

$$365 \equiv 1 \ mod \ 7$$

Multiplicando por el número de años transcurridos

$$183(365) \equiv 183 \ mod \ 7 \equiv 1 \ mod \ 7$$

luego, después de agregar todos los días adicionales, producto de los años bisiestos, tenemos:

$$x \equiv 45 + 1 \ mod\ 7 \equiv 46 \ mod\ 7 \equiv 4 \ mod\ 7$$

Por lo tanto hay un desfase de 4 días en el almanaque del año 1810 con respecto al año 1993. Por comodidad, este desfase lo haremos positivo, $-4 \equiv 3 \ mod\ 7$. Luego el desfase será de tres días contando los días hacia adelante en el tiempo.

Para terminar de resolver el problema, miramos el almanaque de 1993 y vemos que el 19 de abril fue lunes. Luego el 19 de abril de 1810 fue jueves.

De la misma forma como hallamos el día de la semana correspondiente al 19 de abril de 1810, podemos determinar cualquier día de otra fecha en ese año. Basta ubicar la fecha correspondiente en el almanaque de 1993, y entonces agregar tres días más. Es decir, el desfase x da toda la información necesaria. Daremos los desfases para los años en el período de vida del Libertador Simón Bolívar.

Tabla Cronológica

1783	1784	1785	1786	1787	1788	1789	1790	1791	1792
6	1	2	3	5	6	7	1	3	4
1793	1794	1795	1796	1797	1798	1799	1800	1801	1802
4	5	6	1	2	3	4	5	6	7
1803	1804	1805	1806	1807	1808	1809	1810	1811	1812
1	3	4	5	6	1	2	3	4	6
1813	1814	1815	1816	1817	1818	1819	1820	1821	1822
7	1	2	4	5	6	7	2	3	4
1823	1824	1825	1826	1827	1828	1829	1830		
5	7	1	2	3	5	6	7		

Ciclos Lunares

El ciclo lunar o ciclo metónico, es un período igual a 19 años solares. La razón de esto se debe al astrónomo griego Meton (siglo 5 a.c.), quien descubrió que 19 años solares son iguales a 235 meses lunares.

El **mes lunar** o **mes sinódico**, es el intervalo de tiempo entre dos conjunciones consecutivas del sol y la luna (4 fases lunares). Este tiene una duración de 29 días, 12 horas y 44 minutos. En la Iglesia Cristiana hubo necesidad de introducir el ciclo lunar dentro del Calendario, debido a la determinación del Domingo de Pascua, el cual depende de la luna llena, como ya hemos explicado.

Los años del ciclo metónico se llaman **años dorados**. El primer año de un ciclo es aquel en que las fases lunares del mes de enero de dicho año comienzan el 24 de diciembre. Así, por ejemplo en el año 1 de la Era Cristiana se inició un ciclo metónico. Luego en año 1 d.c. tiene número dorado 1, el año 2 d.c. tiene número dorado 2 ,..etc. Luego el año 20 tiene número de oro 1, y asi sucesivamente.

La regla para calcular el número de oro t, de un año x cualquiera es:

$$t \equiv x + 1 \ mod\ 19$$

Por ejemplo 1993 tiene número de oro 18, pues

$$1993 + 1 = 1994 \equiv 18 \ mod\ 19$$

2.4 Trucos de divisibilidad

Existen criterios prácticos para decidir cuándo un número es divisible entre 3,9, 11,$\cdots$ etc. Todos estos criterios están basados en las congruencias y son fáciles de interpretar, una vez vistos los resultados previos, en donde se estudiaron las reglas de manipulación de ecuaciones de congruencias.

Criterio de divisibilidad entre nueve

Proposición 2.4.1 *Un número x es divisible entre nueve si y sólo si la suma de sus dígitos es divisible entre nueve.*

Demostración:

En primer lugar notemos que

$$10 \equiv 1 \ mod\ 9$$

Multiplicando esta ecuación por sí misma tantas veces como se desee

$$10^i \equiv 1 \ mod\ 9 \quad \text{para todo } \ 1 \leq i.$$

Sea ahora x un número positivo cualquiera. Entonces x tiene una descomposición decimal, y por lo tanto existen enteros c_i, $0 \leq i \leq n$, tales que

$$x = c_n 10^n + \ldots c_1 10 + c_0$$

donde $0 \leq c_i \leq 9$, para todo i. Luego

$$x = c_n 10^n + \ldots + c_1 10 + c_0 \equiv c_n + \ldots + c_1 + c_0 \ mod\ 9$$

Como consecuencia de lo anterior, hemos demostrado que x es congruente módulo 9 a la suma de sus dígitos. Entonces x es un múltiplo de 9 si y sólo si la suma de sus dígitos lo es.

Ejemplo: El entero 1575 es divisible entre 9, pues

$$1 + 5 + 7 + 5 = 18 = 2 \times 9.$$

Criterio de divisibilidad entre 3

Proposición 2.4.2 *Un número es divisible entre 3 si y sólo si la suma de sus dígitos es divisible entre 3.*

Veamos ahora otra aplicación práctica de las congruencias, en la obtención de un viejo truco para verificar el resultado de una multiplicación, llamado **Eliminación de los Nueve**. Si se multiplican dos números a y b, para obtener un resultado c, entonces daremos un método para verificar si c es el resultado correcto. Este método falla en un 10 por ciento de los casos, pero sin embargo es apropiado para esta tarea, debido a la simplicidad del mismo.

Eliminación de los nueve

Proposición 2.4.3 *Si en la multiplicación de a por b se obtiene un entero c, entonces al sumar los dígitos de cada una de los tres números se obtienen enteros a', b' y c', los cuales deben satisfacer: $a' \times b' = c'$.*

Daremos un ejemplo práctico para ilustrar este método.

786	$7+8+6=21$	$2+1=3$	3
x219	$2+1+9=12$	$1+2=3$	x3
172134	$1+7+2+1+3+4=18$	$1+8=9$	9

La prueba de la proposición, es una consecuencia del criterio de divisibilidad entre nueve, pues

$$a \equiv a' \ mod\ 9 \quad \text{y} \quad b \equiv b' \ mod\ 9,$$

Luego se tiene

$$ab \equiv a'b' \ mod\ 9$$

o sea

$$c \equiv c' \ mod\ 9.$$

Ejercicios

1) Hallar criterios de divisibilidad para 2 y 5. Justificarlos.

2) Hallar y probar un criterio de divisibilidad para 11.

3) Hallar y probar un criterio de divisibilidad para 7.

4) Existe un método para multiplicar, que fue muy popular en Europa durante la Edad Media, en el cual sólo se requiere la tabla de multiplicación hasta el número cinco. Supongamos que queremos multiplicar 7 por 8. Entonces la diferencia de 8 con 10 es 2 y la diferencia de 7 con 10 es 3. Multiplicando ambas diferencias nos da: $2 \times 3 = 6$. Este es el primer dígito del resultado. Luego a 7 se le resta la diferencia del 8 (o bien a 8 se le resta la diferencia de 7) y en cualquiera de los dos casos nos da 7-3 = 8-2 = 5 . Este es el otro dígito del número buscado. Podemos ilustrar este algoritmo, mediante el diagrama:

Dar una demostración de este algoritmo.

5) Demuestre que el almanaque se repite cada 28 años.

6) Usando la tabla cronológica hallar los días de la semana de las fechas siguientes.

a) 25 de marzo de 1.815
b) 6 de enero de 1.799
c) 24 de diciembre de 1803

7) Demostrar que el error cometido al medir el tiempo con el Calendario Juliano es de un día cada 128 años.

8) Calcular el error que se comete al medir el tiempo con el Calendario Gregoriano.

9) Usando el truco de eliminación de los nueve, verificar las operaciones siguientes.
a) $1.254 \times 456 = 571.824$
b) $6.532 \times 123 = 893.436$
c) $1.223 \times 362 = 442.626$
d) $125 \times 337 = 41.125$

10) Hallar el valor de x que satisfaga
a) $x^2 \equiv -1 \ mod\ 7$
b) $2^x \equiv 1 \ mod\ 5$
c) $x^3 + 4x - 1 \equiv 0 \ mod\ 7$

2.5 Clases de congruencias

Hemos visto que para un número positivo m fijo, la relación módulo m en el conjunto de enteros es de equivalencia. En esta sección, veremos cómo se puede dotar al conjunto de las clases de congruencias de una estructura algebráica.

Supondremos que el lector está familiarizado con los conceptos de **operación binaria, grupo y anillo** . De cualquier forma, daremos un breve repaso a estos conceptos con la finalidad de hacer esta sección autocontenida.

Definición 2.5.1 *Sea A un conjunto no vacío. Una* **operación binaria** *en A es una ley que asocia a cada par de elementos (a, b) de $A \times A$ otro elemento de A el cual será denotado por $a * b$. Esto se simboliza por*

$$* : A \times A \longrightarrow A$$

$$(a, b) \longrightarrow a * b$$

Definición 2.5.2 *Un* **Grupo** *es un conjunto no vacío G, el cual está dotado de una operación binaria $*$, la cual satisface*

1. *Para a y b en G, $a * b$ está en G.*

2. *Para a, b y c en G*

$$(a * b) * c = a * (b * c)$$

3. *Existe un elemento e en G, llamado el elemento neutro de G, el cual satisface:*

$$a * e = e * a = a \quad \textit{para todo } a \textit{ en } G.$$

4. *Para todo a en G, existe un elemento en G, llamado el inverso de a, el cual denotamos por a^{-1}, con la propiedad:*

$$a * a^{-1} = a^{-1} * a = e.$$

Si además de las cuatro propiedades anteriores, el grupo G posee la propiedad adicional

$$a * b = b * a$$

para todo a y b en G, entonces diremos que G es un **grupo abeliano**.

Ejemplo: El conjunto de los números enteros con la suma $(\mathbb{Z}, +)$ es un grupo abeliano.

Ejemplo: El conjunto de las fracciones no nulas bajo el producto, $(\mathbb{Q}^*, .)$ es un grupo abeliano.

Definición 2.5.3 *Sea $\mathbb{R}$ un grupo abeliano con operación *. Diremos que $\mathbb{R}$ es un* **anillo**, *si en $\mathbb{R}$ está definida otra operación $\oplus$, la cual verifica:*

1. *Para a y b en $\mathbb{R}$, $a \oplus b$ está en $\mathbb{R}$.*

2. *para a, b y c en $\mathbb{R}$*

$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

3. Para todos a, b y c en $\mathbb{R}$

$$a \oplus (b * c) = a \oplus b * a \oplus c$$

y

$$(a * b) \oplus c = a \oplus c * b \oplus c$$

Notación: El anillo $\mathbb{R}$ con las dos operaciones *, $\oplus$, se denota por $(\mathbb{R}, *, \oplus)$.

Si además el anillo $\mathbb{R}$ satisface la propiedad

$$a \oplus b = b \oplus a \quad \text{para todo } a, b \text{ en } \mathbb{R},$$

entonces diremos que $\mathbb{R}$ es un **anillo conmutativo**.

Si en $\mathbb{R}$ hay elemento identidad para el producto, es decir un elemento llamado "uno" y denotado por 1, tal que

$$1 \oplus a = a \oplus 1 = a$$

para todo a, diremos que $\mathbb{R}$ es un **Anillo Unitario**.

Ejemplo: *Los Enteros*
El conjunto $\mathbb{Z}$ de los números enteros con la suma y multiplicación, es un anillo conmutativo unitario.

Ejemplo: *Los Polinomios*
El conjunto de todos los **Polinomios** en una variable x con coeficientes enteros, con las operaciones de suma y producto de polinomios, es un anillo conmutativo unitario. Este anillo se denota por $\mathbb{Z}[x]$.

Enteros módulo m

A continuación daremos un ejemplo de anillo, que será de importancia fundamental en todo el desarrollo de la teoría de números. Consideremos un entero positivo m, y sea $\mathbb{Z}_m$ el conjunto de clases de equivalencia módulo m. Entonces hay dos operaciones definidas en $\mathbb{Z}_m$.

1. **Suma módulo** m, definida por
$$[a] + [b] = [a + b]$$
2. **Producto módulo** m, definida por
$$[a] \cdot [b] = [a \cdot b]$$

Antes de pasar a ver las propiedades de este par de operaciones, debemos asegurarnos de que no hay ambigüedades en la definición. Esto es, si sumamos dos clases usando distintos representantes: ¿Se obtendrá el mismo resultado? Es decir, si a_1, a_2, b_1, b_2 son enteros tales que

$$[a_1] = [a_2] \quad \text{y} \quad [b_1] = [b_2]$$

entonces debemos asegurarnos, para evitar dudas, que:

$$[a_1] + [b_1] = [a_2] + [b_2]$$

Si esto se cumple, diremos que la suma módulo m **está bien definida**.

Notemos en primer lugar que si $[a_1] = [a_2]$ entonces

$$a_1 \equiv a_2 \ mod \ m$$

Igualmente, de $[b_1] = [b_2]$ se desprende

$$b_1 \equiv b_2 \ mod \ m$$

Por lo tanto podemos sumar ambas congruencias para obtener

$$a_1 + b_1 \equiv a_2 + b_2 \ mod \ m,$$

lo cual implica

$$[a_1 + b_1] = [a_2 + b_2],$$

luego $[a_1] + [b_1] = [a_2] + [b_2]$.

De igual manera, para el producto tenemos

$$[a_1].[b_1] = [a_2].[b_2].$$

Concluimos de esta manera que la suma y el producto módulo m están bien definidas.

Proposición 2.5.1 *Sea m un entero positivo. Entonces el conjunto $\mathbb{Z}_m$ de las clases de congruencias módulo m, con las operaciones de suma y producto módulo m es un anillo conmutativo con unidad.*

Demostración:

Ejercicio. ♠

Ejemplo: Consideremos $\mathbb{Z}_6$, el anillo de los enteros módulo 6. Podemos construir una tabla para la operación de suma, para lo cual colocaremos todos los elementos de $\mathbb{Z}_6$ en la primera columna y en la primera fila de la tabla

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Ejercicio: Analizar la tabla anterior, verificando cada una de las operaciones y responda a las preguntas

1. ¿Por qué la tabla es simétrica con respecto a la diagonal ?
2. ¿Por qué ningún elemento se repite en una misma columna o fila?
3. ¿Por qué aparece el cero en todas las filas y columnas?

Podemos construir una tabla para el producto módulo 6, de la misma forma como lo hicimos para la suma.

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Si analizamos esta tabla, vemos que en la columna del elemento 2, no aparece el elemento 1. Luego no existe elemento x tal que $[2] \cdot [x] = 1$. Por lo tanto los enteros módulo 6 no forman un grupo bajo el producto, pues el elemento [2] no posee inverso.

Definición 2.5.4 *Un anillo conmutativo con unidad $\mathbb{R}$, en donde todo elemento posee inverso bajo el producto, se llama un* **Cuerpo.**

Observación : Si el anillo conmutativo unitario $\mathbb{R}$ es finito, entonces la existencia de elementos inversos para el producto es equivalente a la ley de cancelación para el producto. La cual establecemos a continuación:

Ley de cancelación para el producto: Si a, b y c son elementos de $\mathbb{R}$ tales que $a \neq 0$, entonces

$$a \cdot b = a \cdot c \quad \text{implica} \quad b = c$$

La prueba de esto se deja como ejercicio para el lector.

Veamos bajo que condiciones sobre m, se cumple la ley de cancelación en $\mathbb{Z}_m$.

Teorema 2.5.1 *Sea a un entero positivo y $(a, m) = d$. Entonces si*

$$ab \equiv ac \ mod \ m,$$

se tiene

$$b \equiv c \ mod \ \frac{m}{d}$$

Demostración:

Tenemos por hipótesis que $m \mid a(b-c)$. Luego m/d divide a $a/d(b-c)$ y además $(\frac{m}{d}, \frac{a}{d}) = 1$. Luego concluimos que m/d divide a $b - c$, de donde se obtiene

$$b \equiv c \ mod \ \frac{m}{d}$$

♠

Ejemplo: Sea la congruencia $3 \times 2 \equiv 3 \times 4 \ mod \ 6$. Notar que $(3, 6) = 3$ y por lo cual se tiene $2 \equiv 4 \ mod \ 2$.

Proposición 2.5.2 *Sea p un primo y a un entero positivo, tal que $(p, a) = 1$, entonces si*

$$ab \equiv ac \; mod \; p, \quad se \; tiene \quad b \equiv c \; mod \; p.$$

Finalmente, podemos caracterizar los anillos $\mathbb{Z}_m$, que son cuerpos.

Teorema 2.5.2 *El anillo de clases de congruencias $\mathbb{Z}_p$ es un cuerpo sí y sólo si p es primo.*

Demostración:

Ejercicio. ♠

Ejercicios

1) Construir tablas para las operaciones de suma y producto módulo 7.

2) Usando las tablas anteriores, resolver la congruencias

1. $2a \equiv 3 \; mod \; 7$
2. $5a \equiv 4 \; mod \; 7$

3) Un elemento $a \neq 0$ en un anillo $\mathbb{R}$, se dice que es un **divisor de cero**, si existe un $b \neq 0$ en $\mathbb{R}$, tal que $a \cdot b = 0$. Demostrar que no hay divisores de cero en Z_p, con p primo.

4) Demuestre que el anillo $\mathbb{Z}_m$ tiene exactamente m elementos.

5) Demuestre que en un grupo siempre se puede resolver la ecuación: $a * x = b$.

6) Sea $\mathbb{R}$ un anillo y a, b y c elementos de $\mathbb{R}$. ¿Bajo que condiciones sobre estos elementos, se puede resolver la ecuación: $a \cdot x + b = c$?

7) Demuestre que si $f(x)$ y $h(x)$ son dos polinomios con coeficientes reales, se cumple que

$$f(x)h(x) = h(x)f(x).$$

8) Demuestre que no existe divisores de cero en el anillo de polinomios sobre los reales.

9) Probar que $[a], [b]$ y $[c]$ son tres clases de congruencia módulo m, se cumple que

$$[a] + ([b] + [c]) = ([a] + [b]) + [c].$$

10) Si p es un número primo probar que $\mathbb{Z}_p$ es un cuerpo.

11) Sea A el conjunto de los números reales de la forma $a + b\sqrt{2}$, con a y b números racionales. Probar que A es un cuerpo con las operaciones de suma y producto de números reales.

12) Probar que en la tabla de operación de un grupo no pueden haber elementos repetidos en una misma fila o columna.

2.6 Ecuaciones lineales de congruencia

Una ecuación del tipo

$$a \cdot x \equiv b \; mod \; m \tag{2.1}$$

se llama **ecuación lineal de congruencia**.

Observación: Si x_0 es solución de (2.1), y x_1 es otro entero tal que $x_1 \equiv x_0 \; mod \; m$, entonces x_1 también será solución de la ecuación. Así pues, si (2.1) posee solución, entonces posee infinitas. Sin embargo sólo nos interesan aquellas soluciones que no sean congruentes entre si.

Volviendo a la ecuación anterior, podemos expresarla como

$$a \cdot x - m \cdot y = b \tag{2.2}$$

donde y es un entero a determinar.

Una ecuación del tipo (2.2) se denomina **ecuación lineal diofántica** en las variables x e y. Se supone que las soluciones de esta ecuación son números enteros.

Diofantos de Alejandría fue uno de los grandes matemáticos griegos y escribió sus obras a mediados del siglo 3 d.c. La más importante es la *Aritmética*, que consistía en el estudio de resolución de ecuaciones, como por ejemplo la ecuación $Ax^2 + C = y^2$.

Ejemplo:
Resolver

$$7 \cdot x + 15 \cdot y = 12$$

Solución:

Usaremos el método de Euler, que consiste en despejar una de las incógnitas con menor coeficiente, en función de la otra.

Esto nos conduce a establecer una ecuación diofántica con coeficientes menores.

Se tiene entonces

$$x = \frac{12 - 15 \cdot y}{7} = 1 - 2 \cdot y + \frac{5 - y}{7}$$

Si se requiere que x e y sean enteros, se debe tener

$$z = \frac{5 - y}{7} \quad \textit{entero.}$$

Luego

$$y = 5 - 7 \cdot z$$

Dándole valores enteros arbitrarios a z, podemos obtener valores enteros de x e y, que cumplen la ecuación original. Expresando x e y en función de z se deduce

$$x = -9 + 15 \cdot z$$

$$y = 5 - 7 \cdot z.$$

Siendo z cualquier entero. Por ejemplo, haciendo $z = 0$ se tiene $x = -9$, $y = 5$, lo cual nos da una solución a la ecuación.

Como veremos enseguida, la ecuación lineal diofántica siempre se puede resolver si se cumplen ciertas condiciones sobre los coeficientes a, b y c.

Teorema 2.6.1 *La ecuación*

$$ax + by = c \tag{2.3}$$

tiene solución si y sólo si $d \mid c$, *donde* $d = (a, b)$.

Demostración:

Notemos en primer lugar que $d \mid a$, y $d \mid b$. Por lo tanto, si la ecuación (2.3) tiene solución (x, y) se tiene que $d \mid ax + by$, y luego $d \mid c$.

Recíprocamente, supongase que $d \mid c$. Dividiendo entre d la ecuación original, nos da

$$a'x + b'y = c' \tag{2.4}$$

donde $a' = a/d$, $b' = b/d$ y $c' = c/d$. Es claro que si (2.4) tiene solución, entonces (2.3) también posee solución y viceversa. Luego ambas ecuaciones son equivalentes.

Notemos que $(a', b') = 1$, y por lo tanto existen enteros x'_0 e y'_0 tales que

$$a'x'_0 + b'y'_0 = 1$$

Luego es fácil verificar que $x_0 = c'x'_0$ e $y_0 = c'y'_0$ son soluciones de (2.4) y por ende soluciones de (2.3).

Teorema 2.6.2 *Si la ecuación lineal diofántica (2.3) posee solución y* (x_0, y_0) *es una solución particular, entonces toda otra solución* (x, y) *es de la forma*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

donde t *es cualquier entero.*

Demostración:

En primer lugar, probaremos que x e y son solución. En efecto

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + by_0 = c$$

Por otro lado si (x, y) es cualquier solución de (2.3), también lo será de (2.4) y en consecuencia

$$a'(x - x_0) + b'(y - y_0) = c' - c' = 0$$

de donde

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

De acá se deduce $a' \mid b'(y - y_0)$ y por lo tanto $a' \mid (y - y_0)$. Luego $y = y_0 + a't$, donde t es un entero. Igualmente, se verifica $x = x_0 + b's$, con s entero.

Probaremos que $s = -t$, para lo cual sustituimos la solucion (x, y) en (2.4)

$$a'(x_0 + b's) + b'(y_0 + a't) = c'$$

$$a'x_0 + b'y_0 + a'b'(s + t) = c'$$

como (x_0, y_0) es solución de (2.4) se tiene $a'x_0 + b'y_0 = c'$, y por lo tanto

$$c' + a'b'(s + t) = c'$$

o sea

$$a'b'(s + t) = 0$$

de donde $s = -t$. Con esto termina la demostración.

♠

Teorema 2.6.3 *La ecuación lineal de congruencia*

$$ax \equiv b \ mod \ m \tag{2.5}$$

posee solución si y sólo si $d \mid b$, donde $d = (a, m)$. Si x_0 es una solución particular de (2.5), entonces la solución general viene dada por

$$x \equiv x_0 \ mod \ \frac{m}{d}.$$

Demostración:

Podemos expresar la ecuación anterior como

$$ax - my = b \tag{2.6}$$

De acuerdo al teorema anterior, sabemos que (2.6) posee solución y además la solución general para la x viene expresada mediante:

$$x = x_0 + \frac{m}{d}t.$$

Para finalizar la demostración, observemos que las d soluciones

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}$$

son todas distintas módulo m. ♠

Ejemplo:
Resolver

$$30x \equiv 15 \ mod \ 21$$

Solución:

Obsérvese que $(30, 21) = 3$, y 3 divide a 15. Luego la ecuación tiene solución. El número de soluciones módulo 21 será igual a $(21, 30) = 3$.

Con la finalidad de hallar una solución particular, procederemos a dividir entre 3 la ecuación. Luego

$$10x \equiv 5 \ mod \ 21$$

esto es

$$3x \equiv 5 \ mod \ 7$$

Por simple inspección, calculamos una solución $x \equiv 4 \ mod \ 7$. Luego las tres soluciones distintas módulo 21 son: 4, 11 y 18.

Ejemplo:

Resolver

$$238x + 125y = 31$$

Solución:

En este ejemplo se puede reducir el tamaño de los coeficientes, mediante un cambio de variables. Podemos reescribir la ecuación anterior

$$125(y + 2x) - 12(x + 2) = 7$$

Empleamos ahora el siguiente cambio de variables

$$X = x + 2, \quad Y = y + 2x$$

Luego la ecuación original se transforma en

$$125Y - 12X = 7$$

Resolviendo tenemos

$$X = \frac{125Y - 7}{12} = 10Y + \frac{5Y - 7}{12}$$

Nuevamente, haciendo el cambio de variable

$$z = \frac{5Y - 7}{12}$$

de donde

$$Y = \frac{12z + 7}{5} = 2z + 1 + \frac{2z + 2}{5}$$

Luego $\dfrac{2z + 2}{5}$ es un entero y por lo tanto hacemos $z = -1$.

De aquí obtenemos los resultados

$$Y = -1, \quad X = -11$$

volviendo al cambio de variables

$$y = 15, \quad x = -13$$

Luego la solución de la ecuación original viene expresada por

$$x = -13 + 125t, \quad y = 15 - 238t$$

Estudiemos ahora el problema de resolver una ecuación de congruencia con más de una indeterminada.

Ejemplo:
Resolver

$$3x + 4y \equiv 11 \ mod \ 14 \tag{2.7}$$

En primer lugar, observamos que $14 = 7 \cdot 2$. Luego es posible trabajar con módulos 7 ó 2, para hallar soluciones de (2.7). Escogemos el 2 por ser menor. Luego tomando la misma ecuación módulo 2 se obtiene

$$3x + 4y \equiv 11 \ mod \ 2$$

o sea

$$3x \equiv 1 \ mod \ 2$$

De esta ecuación provienen 7 soluciones distintas módulo 14 para x, las cuales son: 1, 3, 5, 7, 9, 11 y 13. Al sustituir cada una de éstas en la ecuación original, se obtendrán las correspondientes soluciones para la y.

Por ejemplo, si se considera $x \equiv 1 \ mod \ 14$, se tendrá

$$3x + 4y \equiv 11 \ mod \ 14$$

o bien

$$4y \equiv 8 \ mod \ 14$$

Notemos que $(14, 2) = 2$, luego podemos simplificar:

$$2y \equiv 4 \ mod \ 7$$

Luego las soluciones de y módulo 14 son 2 y 9.

Usaremos pares ordenados para indicar las soluciones de la ecuación (2.7), donde la primera componente indica la x y la segunda indica la y. De esta forma, se obtienen las soluciones $(1, 2)$ y $(1, 9)$.

Las restantes soluciones son:

$$(3,4),\ (3,11),\ (5,6),\ (5,13),\ (7,1),\ (7,8),$$
$$(9,3),\ (9,10),\ (11,5),\ (11,12),\ (13,7),\ (13,14).$$

Teorema 2.6.4 *La congruencia*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \equiv c\ mod\ m$$

es soluble si y sólo si $d \mid c$, *donde* $d = (a_1, a_2, \ldots, a_n, m)$.

El número de soluciones distintas módulo m *es* dm^{n-1}.

Demostración:

Haremos la demostración para el caso $n = 2$. El caso general se deduce de este caso particular y del principio de inducción.

Consideremos entonces

$$a_1x + a_2y \equiv c\ mod\ m \tag{2.8}$$

donde $(a_1, a_2, m) = d$ y $d \mid c$.

Es fácil ver que la condición $d \mid c$ es necesaria para la existencia de la solución. Probaremos que esta condición es también suficiente.

A tal efecto, sea $(a_2, m) = d'$. Luego de (2.8) obtenemos

$$a_1x \equiv c\ mod\ d' \tag{2.9}$$

Notemos que $(d', a_1) = ((a_2, m), a_1) = d$, y $d \mid c$. Luego (2.9) posee d soluciones distintas módulo d', de acuerdo al teorema 2.6.3. Estas d soluciones, generan $d \cdot m/d'$ soluciones distintas módulo m para x.

Para cada solución x, se reemplaza su valor en la ecuación (2.8) para obtener

$$a_2 y \equiv c - a_1 x \ mod \ m$$

Teniendo en cuenta que: $(m, a_2) = d'$, y además: $d' \mid c - a_1 x$, se deduce entonces que la ecuación anterior posee d' soluciones distintas para y módulo m.

Contando el número de soluciones de (2.8), se tendrá la ecuación

$$S = S_x \times \ S_y$$

donde S = número de soluciones de (2.8), S_x = número de soluciones para x y S_y = número de soluciones para y. Luego

$$S = d \ \frac{m}{d'} \ d' = d.m$$

2.7 Teorema Chino del Resto

El problema de resolver la congruencia

$$ax \equiv b \ mod \ m \tag{2.10}$$

puede ser bastante laborioso si m es grande, debido al número de calculos requeridos, cuando esta se resuelve usando el método de la sección anterior. Si m se factoriza como un producto de enteros $m_1.m_2 \ldots m_n$ entonces la ecuación anterior es equivalente a las ecuaciones

$$ax \equiv b \ mod \ m_i, \qquad 1 \leq i \leq n$$

Teorema 2.7.1 *Sean $m_1, m_2, \ldots, m_n$ enteros positivos. Entonces el sistema*

$$\begin{cases} ax & \equiv & b \ mod \ m_1 \\ & \vdots & \\ ax & \equiv & b \ mod \ m_n \end{cases}$$

es equivalente a la ecuación

$$ax \equiv b \ mod \ [m_1, m_2, \ldots, m_n]$$

Demostración:

Notemos que para todo i, se tiene $m_i \mid ax - b$, por hipótesis, luego $ax - b$, es múltiplo común de los m_i y por lo tanto $[m_1, \ldots, m_n]$ divide a $ax - b$. Luego

$$ax \equiv b \ mod \ [m_1, \ldots, m_n].$$

Recíprocamente, es fácil ver que toda solución de la ecuación satisface el sistema, con lo cual se da fin a la prueba.

♠

Observación: Si los m_i son primos relativos por pareja, esto es,

$$(m_i, m_j) = 1$$

para todo par de enteros $i \neq j$,

entonces se tiene

$$[m_1, \ldots, m_n] = m_1 \ldots m_n.$$

Así pues, tenemos el siguiente resultado

Teorema 2.7.2 *Si m se factoriza*

$$m = p_1^{\alpha_1}.p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

entonces la ecuación $ax \equiv b \ mod \ m$ es equivalente al sistema de n ecuaciones

$$ax \equiv b \ mod \ p_i^{\alpha_i}, \quad 1 \leq i \leq n$$

Ejemplo:
Resolver

$$7x \equiv 6 \ mod \ 100$$

Solución:

Descomponiendo a 100 como producto de primos, nos da $100 = 2^2 5^2$, luego la ecuación es equivalente al sistema

$$7x \equiv 6 \ mod \ 25$$

$$3x \equiv 2 \ mod \ 4$$

La primera ecuación tiene solución

$$x \equiv 8 \ mod \ 25,$$

o sea $x = 8, 33, 58, 83, \ldots$.

La segunda ecuación tiene solución

$$x \equiv 2 \ mod \ 4,$$

esto es $x = 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, \ldots$.

Luego la solución común viene expresada por

$$x \equiv 58 \ mod \ 100$$

Ejemplo:

Ahora planteamos un problema de la antigua China, que data del año 1275 d.c.

"Hallar un número tal que, al ser dividido por siete da uno como residuo, al ser dividido por ocho da dos como residuo y al ser dividido por nueve da tres como residuo".

Solución:

Podemos plantear el problema en términos de congruencias de la siguiente manera; sea x el número buscado, entonces

$$\begin{cases} x & \equiv & 1 \ mod \ 7 \\ x & \equiv & 2 \ mod \ 8 \\ x & \equiv & 3 \ mod \ 9 \end{cases}$$

De la primera ecuación obtenemos

$$x = 1 + 7k$$

Sustituyendo en la segunda ecuación

$$1 + 7k \equiv 2 \ mod \ 8$$

de donde

$$7k \equiv 1 \ mod \ 8$$

Luego

$$k \equiv 7 \ mod \ 8,$$

y por lo tanto $k = 7 + 8l$. Sustituyendo en la expresión de x nos da: $x = 50 + 56l$. Este último valor de x lo sustituimos en la tercera ecuación para obtener

$$50 + 56l \equiv 3 \ mod \ 9$$

y después de reducir módulo 9 nos queda: $l = 8 + 9j$.

Finalmente, si se remplaza el valor de l en la expresión de x produce

$$x = 50 + 56(8 + 9j) = 498 + 504j$$

de donde se concluye

$$x \equiv 498 \ mod \ 504$$

Proposición 2.7.1 *Sean m_1 y m_2 enteros primos relativos. Entonces existen enteros x_0 y x_1 tales que*

$$\begin{array}{ll} x_0 \equiv 1 \ mod \ m_1 & x_0 \equiv 0 \ mod \ m_2 \\ x_1 \equiv 0 \ mod \ m_1 & x_1 \equiv 1 \ mod \ m_2 \end{array} \tag{2.11}$$

Demostración:

Sabemos que existen enteros s y t tales que

$$s \cdot m_1 + t \cdot m_2 = 1$$

Luego $s \cdot m_1 \equiv 1 \ mod \ m_2$ y $s \cdot m_1 \equiv 0 \ mod \ m_1$. Similarmente $t \cdot m_2 \equiv 1 \ mod \ m_1$ y $t \cdot m_2 \equiv 0 \ mod \ m_2$. Tomar entonces $x_0 = t \cdot m_2$ y $x_1 = s \cdot m_1$.

♠

Proposición 2.7.2 *Sean m_1 y m_2 enteros primos relativos. Entonces dados dos enteros cualesquiera a y b, existe un entero x que satisface*

$$x \equiv a \ mod \ m_1$$

$$x \equiv b \ mod \ m_2$$

Demostración:

Tomar $x = a \cdot x_0 + b \cdot x_1$, donde x_0 y x_1 satisfacen la condición (2.11)

♠

Teorema 2.7.3 *(Teorema Chino del Resto)*
Sean $m_1, \ldots, m_n$ enteros positivos, primos relativos por parejas. Entonces si $a_1, \ldots, a_n$ son enteros cualesquiera, el sistema

$$\begin{cases} x & \equiv a_1 \mod m_1 \\ & \vdots \\ x & \equiv a_n \mod m_n \end{cases}$$

posee solución. Además si $m = m_1 \cdots m_n$, cualquier par de soluciones son congruentes módulo m.

Demostración:

Usaremos inducción sobre n. Para $n = 1$ el teorema es cierto. Supongase que el sistema

$$\begin{cases} x & \equiv a_1 \mod m_1 \\ & \vdots \\ x & \equiv a_{n-1} \mod m_{n-1} \end{cases}$$

posee solución única x_0 módulo $m' = m_1 \cdot m_2 \cdots m_{n-1}$.

Entonces el sistema original se puede reducir a resolver

$$x \equiv x_0 \mod m'$$

$$x \equiv a_n \mod m_n$$

Tenemos entonces que $(m_n, m') = (m_n, m_1 \ldots . m_{n-1}) = 1$. Luego podemos aplicar la proposición anterior para hallar la solución buscada, la cual será única módulo $m_1 \cdots m_n$, por hipótesis de inducción.

Aplicación del teorema chino en cronología

Una de las medidas más usadas en la cronología histórica es la de los **días julianos**. Los días julianos tienen la misma duración que los días

solares, sin embargo éstos se cuentan a partir del primero de enero del 4713 a.c., el cual es el día juliano 1, y de allí en adelante se enumeran los días en sucesión creciente.

Este sistema fue ideado por **Joseph Justus Scaliger** de Leyden, y apareció por primera vez en su obra "*De emendatione temporum*" (París 1583).

Estos días julianos se agrupan en períodos de 7980 años. Cada uno de estos períodos se denomina **Ciclo Juliano o Período Juliano**. La razón para elegir semejante número, la veremos a continuación.

Tenemos que $7980 = 28 \times 19 \times 15$ y cada uno de estos factores tiene un significado muy especial dentro de los calendarios de distintas cronologías

El número 28 corresponde al llamado **Ciclo Solar** de 28 años. Este es el ciclo más pequeño en el cual los días de la semana y las fechas del calendario se repiten. El primer año de un ciclo solar es aquel, en donde el día primero de enero es lunes. Por ejemplo, el año 1560 tiene año solar 1.

El número 19 corresponde al **Ciclo Metónico o Ciclo Lunar**, el cual dura 19 años. Este es el menor ciclo en el cual las fases de la luna se repiten en las mismas fechas del calendario. Este proviene del astrónomo griego Meton (siglo V a.c.), quién descubrió que 19 años solares corresponden exactamente a 235 lunaciones o meses lunares. Los años del ciclo metónico se llaman **Años Dorados**. Este sistema fue introducido por el Emperador Dionisio Exigus en el año 533 d.c. y este año tiene año dorado 1.

Finalmente, el número 15 corresponde a otro ciclo, el cual no tiene nada que ver con astronomía. Se trata del ciclo de recolección de impuestos en la antigua Roma que constaba de 15 años y se llama la **indicción**. Este ciclo fue introducido por el Emperador Constantino en el año 313 d.c. correspondiendo a este año el primer año de dicho ciclo.

La idea de Scaliger era usar un sistema de cronología que incluyera todos estos ciclos. Esto permitiría calcular fácilmente una fecha determinada al pasar de un sistema a otro. El problema entonces era

escoger una fecha apropiada para iniciar la cuenta de los años julianos. Se necesitaba un año x de la historia, tal que en ese año se diera inicio a los tres ciclos. Esto es, x debe tener

$$\begin{array}{c}\text{Año solar} = 1\\ \text{Año dorado} = 1\\ \text{Año de indicción} = 1\end{array}$$

Usando congruencias, se debe tener el sistema

$$\begin{cases} x \equiv 1560 \mod 28 \\ x \equiv 532 \mod 19 \\ x \equiv 313 \mod 15 \end{cases}$$

Reduciendo esto se tiene

$$\begin{cases} x \equiv 20 \mod 28 \\ x \equiv 0 \mod 19 \\ x \equiv 13 \mod 15 \end{cases}$$

Nótese que (28, 27) = 1, (28,15) = 1 y (15,19) = 1. Luego por el Teorema Chino del Resto, el sistema anterior posee solución.

A fin de determinar el valor de x, comenzaremos por usar la primera ecuación. Luego

$$x = 20 + 28k \quad \text{con } k \text{ entero.}$$

Usando la segunda ecuación nos queda

$$20 + 28k \equiv 0 \mod 19$$

$$1 + 9k \equiv 0 \mod 19$$

$$9k \equiv 18 \mod 19$$

de donde

$$k \equiv 2 \mod 19$$

Luego

$$k = 2 + 19s$$

y por lo tanto volviendo a x en la última ecuación tenemos

$$76 + 532s \equiv 13 \ mod \ 15$$

$$1 + 7s \equiv 13 \ mod \ 15$$

luego, $7s \equiv 12 \ mod \ 15$, de donde $s \equiv 6 \ mod \ 15$. Por lo tanto $s = 6+15t$.

Nuevamente, si reemplazamos este valor en la expresión para x nos da

$$x = 76 + 532(6 + 15t) = 326 + 7980t$$

Luego la solución viene dada por

$$x \equiv 3268 \ mod \ 7980$$

Sin embargo, descartamos el año 3268 por ser del futuro y buscamos el año y en que se inició el período juliano anterior. Esto es

$$y = 3268 - 7980 = -4712$$

En el calendario gregoriano, el año -4712 corresponde al 4713 a.c. (no hay año 0) y éste se toma como el año 1 juliano.

Ejemplo: Conociendo el año juliano de un año cualquiera, podemos calcular su año solar, dorado y de indicción; basta tomar los restos de la división del número entre 28, 19 y 15 respectivamente. Por ejemplo para buscar el año juliano de 1993, el cual llamaremos x, hacemos

$$x = 4713 + 1993 = 6706$$

Luego dividimos a 6706 entre 28, 19 y 15 respectivamente para obtener los restos que nos dan toda la información. Por lo tanto

Año solar de 1993 = 14
Año dorado de 1993 = 18
Año de indicción de 1993 = 1

Ejercicios

1) Resolver

$$238x + 133y = 31$$

2) Resolver

$$15x + 30y = 720$$

3) Resolver

$$7x + 11y = 150$$

4) Resolver las ecuaciones de congruencia.
   a) $12x \equiv 7 \ mod\ 17$
   b) $11x \equiv 7 \ mod\ 84$
   c) $18x \equiv 1 \ mod\ 25$

5) Resuelva el sistema

$$\begin{cases} x & \equiv 1 & mod\ 2 \\ x & \equiv 2 & mod\ 3 \\ x & \equiv 3 & mod\ 5 \\ x & \equiv 5 & mod\ 7 \end{cases}$$

6) Resuelva la congruencia

$$2x + 3y \equiv 15 \ mod\ 16$$

7) Hacer una tabla en donde aparezcan los años solares, dorados y de indicción para el período comprendido entre 1800 y 1850.

8) Demostrar que si x_0 es un entero y $d|m$, entonces los d enteros

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}$$

son todos diferentes módulo m.

9) Un comerciante compró un lote de juguetes de dos tipos distintos por Bs. 50.000. El primer tipo cuesta Bs. 1.950 por unidad, y el segundo tipo cuesta Bs. 770. ¿Qué cantidad de juguetes de cada tipo compró el comerciante?.

10) Resolver

$$1050x + 6y + 462z \equiv 6 \ mod \ 12$$

11) En X se celebraron eleciones para elegir el Presidente en 1994. En 1992 se realizaron elecciones para elegir gobernadores. Si el período de mando de los presidente es de 5 años, y el de los gobernadores de 8, entonces determine en qué año coincidirán ambas elecciones.

Capítulo

3

Congruencias de Grado Superior

3.1 Introdución

En el capítulo anterior vimos cómo resolver congruencias del tipo

$$ax \equiv b \; mod \; m$$

donde a, b y m son enteros $m > 1$, y $(a, b) = 1$.

En este capítulo discutiremos un nuevo enfoque de este problema, al considerar esta ecuación dentro del anillo de enteros módulo m. Sabemos que a posee un inverso multiplicativo, a^*, con la propiedad

$$a \cdot a^* = 1$$

y por lo tanto se puede multiplicar la ecuación original por a^*, a fin de resolver en términos de x, esto es

$$x \equiv a^* b \; mod \; m$$

Veremos cómo se pueden obtener inversos multiplicativos, mediante el teorema de Euler, lo cual nos permite resolver una gran cantidad de problemas relativos a las congruencias lineales y de grado superior. Como consecuencia del Teorema de Euler, se obtiene el famoso Teorema de Fermat (Pequeño teorema), que establece la identidad

$$x^{p-1} \equiv 1 \; mod \; p$$

válida para todo entero x, con $(x, p) = 1$

Finalmente, se estudian las congruencias polinomiales módulo un entero m. En el caso de ser m un primo se dan una serie de resultados interesantes sobre la factorización y el cálculo de raíces de polinomios.

3.2 La función φ de Euler

Definición 3.2.1 *Sea m un entero positivo. Un* **sistema reducido de residuos** *módulo m, es un conjunto de enteros $a_1, \cdots, a_n$ tales que:*

i) Los a_i son incongruentes módulo m.

ii) Para todo i se tiene $(a_i, m) = 1$.

iii) Si a es un entero cualquiera, tal que $(a, m) = 1$, entonces existe un a_i, tal que $a \equiv a_i \ mod \ m$.

Ejemplo 1:

Un sistema reducido módulo 6, viene expresado por $\{1, 5\}$.

Notemos que las propiedades *i)* y *ii)* ciertamente se satisfacen. Si a es un entero tal que $(a, 6) = 1$, entonces aplicando el algoritmo de la división, se tiene enteros q y r, tales que $a = 6q + r$, donde $0 \leq r < 6$. Por otro lado, $(a, 6) = (6q + r, 6) = (r, 6) = 1$. Luego $r = 1$ ó $r = 5$, lo cual implica

$$a \equiv 1 \ mod \ 6 \quad \text{ó} \quad a \equiv 5 \ mod \ 6$$

Luego *iii)* también se cumple en este ejemplo.

Utilizando un razonamiento análogo, en el caso general, se puede probar:

Teorema 3.2.1 *El conjunto de enteros*

$$A = \{x \mid 0 \leq x < m \ \text{ y } \ (x, m) = 1\}$$

es un sistema reducido de residuos módulo m.

Observación: El teorema anterior demuestra la existencia de un sistema reducido de residuos, para cualquier entero m. Sin embargo existen otros sistemas, además de este dado arriba. Por ejemplo $\{1, 5\}$ y $\{7, 11\}$ son ambos sistemas de residuos módulo 6.

Una pregunta natural es la siguiente: ¿Todo sistema reducido posee el mismo número de elementos? La respuesta a esto es afirmativa, como se verá más adelante.

Definición 3.2.2 *La función φ de Euler, aplicada al entero positivo m se define por*

$$\varphi(m) = |A|$$

En otras palabras, $\varphi(m)$ es el número de enteros positivos mayores o iguales a uno, y menores que m, los cuales son primos relativos con m.

Teorema 3.2.2 *Todo sistema reducido de residuos módulo m, posee $\varphi(m)$ elementos.*

Demostración:

Sea $r_1, \cdots, r_n$ un sistema reducido de residuos módulo m. Probaremos que existe una correspondencia biyectiva entre el conjunto B formado por los r_i y el conjunto A definido previamente.

En efecto, si $x \in A$, se tiene que $(x, m) = 1$ y por ser B un sistema reducido, existe un elemento r_i en B, tal que $x \equiv r_i \ mod \ m$. Por lo tanto definimos

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longrightarrow r_i \end{aligned}$$

Es claro que la función f está bien definida, pues a cada x en A se le puede asignar mediante esta regla un único elemento en B. Seguidamente, probaremos que f es inyectiva y sobreyectiva, con lo cual habremos demostrado que A y B tienen el mismo número de elementos.

Para demostrar la inyectividad, supóngase que x_1 y x_2 son dos elementos en A que satisfacen $f(x_1) = f(x_2)$.

Luego existe un j, $(1 \leq j \leq n)$, tal que

$$\begin{aligned} x_1 &\equiv r_j \ mod \ m \\ x_2 &\equiv r_j \ mod \ m, \end{aligned}$$

lo cual implica $x_1 \equiv x_2 \ mod \ m$. Esto último sucede si y sólo si $x_1 = x_2$.

Para demostrar la sobreyectividad, sea r_i un elemento cualquiera de B. Luego se verifica $(r_i, m) = 1$. Por ser A un sistema reducido, existe un x en A tal que $r_i \equiv x \ mod \ m$, por lo cual $f(x) = r_i$. ♠

Veamos a continuación una tabla con algunos valores de la función φ de Euler.

m	$\varphi(m)$
2	1
3	2
4	2
5	4
6	2

m	$\varphi(m)$
7	6
8	4
9	6
10	4
11	10

m	$\varphi(m)$
12	4
13	12
14	6
15	8
16	8

m	$\varphi(m)$
17	16
18	6
19	18
20	8
21	12

Observando la presente tabla, notamos que $\varphi(m)$ es par, para todo $m \geq 3$. Esto será probado de manera general más adelante. También es evidente que si p es primo, entonces $\varphi(p)$ es igual a $p - 1$. Nuestra próxima meta, será obtener una fórmula para calcular la función de Euler de un número compuesto, la cual va a depender de la factorización de dicho número. Es decir, si m se expresa como un producto de primos $p_1 \cdots p_n$, entonces $\varphi(m)$ se expresará en función de $p_1, \cdots, p_n$.

El primer paso en este proceso viene dado por el siguiente:

Teorema 3.2.3 *Si p es primo y $\alpha \geq 1$, entonces*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Demostración:

Recordemos que $\varphi(p^\alpha)$ es el número de enteros positivos menores o iguales que p^α, y que son primos relativos con p^α. Podemos contar los enteros positivos menores que p^α que no son primos relativos con el. Una lista de estos enteros es la siguiente:

$$p, 2p, 3p, \cdots, (p-1)p, p^2, 2p^2, \cdots, p^{\alpha-1}p$$

vemos que hay entonces $p^{\alpha-1}$ de ellos, luego restando este número del total de enteros positivos menores que p^{α}, obtenemos por lo tanto $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$. ♠

Ejemplo 2:

Por intermedio del teorema anterior podemos calcular la función de Euler sobre una cantidad infinita de números, por ejemplo

$$\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 34.$$

Teorema 3.2.4 *Sean m y n son dos enteros positivos tales que $(m, n) = 1$. Se tiene entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demostración:

Definimos los siguientes conjuntos

$$\begin{aligned} A_n &= \{x | 1 \leq x < n | (x, n) = 1\} \\ A_m &= \{x | 1 \leq x < m | (x, m) = 1\} \\ A_{mn} &= \{x | 1 \leq x < mn | (x, mn) = 1\} \end{aligned}$$

La razón de definir estos tres conjuntos se debe a que $|A_n| = \varphi(n)$, $|A_m| = \varphi(m)$ y $|A_{mn}| = \varphi(mn)$. La idea de la demostración consiste en probar

$$|A_{mn}| = |A_m \times A_n| = |A_n||A_m|,$$

de lo cual se deduce $\varphi(mn) = \varphi(m)\varphi(n)$.

Comenzaremos por definir una función

$$f : A_{mn} \longrightarrow A_n \times A_m$$

de la forma siguiente:

Para cada $x \in A_{mn}$, se cumple $(x, mn) = 1$, de donde $(x, m) = 1$ y $(x, n) = 1$. Luego, existen elementos únicos $r \in A_n$ y $h \in A_m$ tales que $x \equiv r \ mod \ n$ y $x \equiv h \ mod \ m$.

Definimos entonces $f(x) = (r, h) \in A_n \times A_m$. Es claro que f está bien definida.

Además, f es inyectiva, si $f(x) = f(y)$ para algunos enteros x, y en A_{mn}, se tendrá que existen enteros r, h tales que x e y son ambos soluciones del sistema:

$$Z \equiv r \ mod \ n,$$
$$Z \equiv h \ mod \ m.$$

De acuerdo al teorema 3.2.3, el cual afirma la unicidad módulo mn de la solución de este sistema, se tendrá entonces:

$$x \equiv y \ mod \ mn$$

lo cual implica que $x = y$. Por lo tanto f es inyectiva.

Finalmente, para probar la sobreyectividad de f, tomemos un elemento $(i, j) \in A_n \times A_m$. Nuevamente, usamos el teorema 3.2.3 para garantizar la existencia de una solución del sistema

$$Z \equiv i \ mod \ n,$$
$$Z \equiv j \ mod \ m.$$

la cual denotaremos por x. De las dos condiciones $(i, n) = 1$ y $(j, m) = 1$ se deduce que $(x, mn) = 1$, luego $x \in A_{mn}$ y además $f(x) = (i, j)$. Como consecuencia de esto, se ha demostrado que f es sobreyectiva.

Al ser f biyectiva queda probado que

$$|A_{mn}| = |A_n \times A_m|$$

y de esto se deduce:

$$\varphi(mn) = \varphi(m)\varphi(n).$$

♠

Ejemplo 3:

A la luz de los resultados anteriores, nos es permitido ahora calcular la función de Euler para cualquier entero, una vez que se conozca su factorización prima.

Por ejemplo:

$$\begin{aligned}\varphi(600) &= \varphi(2^3 \cdot 3 \cdot 5^3) \\ &= \varphi(2^3)\varphi(3)\varphi(5^3) \\ &= (2^3 - 2^2)(3-1)(5^3 - 5^2) \\ &= 4 \cdot 2 \cdot 20 \\ &= 160\end{aligned}$$

Corolario 3.2.1 *Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, donde los p_i son primos distintos se tendrá entonces:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right)$$

Demostración:

Ejercicio.

3.3 Funciones Multiplicativas

Existen muchas funciones en teoría de números que satisfacen propiedades similares a la función de Euler, como la establecida en el teorema 3.2.4, esto es $\varphi(mn) = \varphi(m)\varphi(n)$ cuando m y n son primos relativos. En esta sección se estudiaran una serie de funciones que cumplen estas y otras propiedades interesantes.

A lo largo de este capítulo, $\mathbb{Z}^+$ denotará el conjunto de los enteros positivos.

Definición 3.3.1 *Una función* $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ *se llama* **función aritmética**.

Definición 3.3.2 *Una función aritmética* f *se dice* **multiplicativa**, *si satisface*

$$f(mn) = f(m)f(n),$$

cada vez que $(m, n) = 1$.

Definición 3.3.3 *Una función aritmética se dice* **totalmente multiplicativa** *si satisface*

$$f(mn) = f(m)f(n),$$

para cualquier par de enteros m *y* n.

Ejemplo 4:

Las funciones siguientes son multiplicativas:
a) La función φ de Euler.
b) La función constante $f(n) = 1$, para todo $n \in \mathbb{Z}^+$.
c) La función idéntica $f(n) = n$, para todo $n \in \mathbb{Z}^+$.
Las dos últimas son totalmente multiplicativas, pero la primera no lo es.

Existen otras funciones multiplicativas, de gran utilidad, como lo son:
$d(n)$ = número de divisores positivos de n.
$\sigma(n)$= suma de los divisores positivos de n.

Ejemplo 5:

Podemos calcular algunos valores de estas funciones y expresarlos mediante una tabla:

n	$d(n)$	$\sigma(n)$
2	2	3
3	2	4
4	3	7
5	6	6
6	4	12
7	2	8
8	4	15
9	3	13
10	4	18
11	2	12

n	$d(n)$	$\sigma(n)$
12	6	28
13	2	14
14	4	24
15	4	24
16	5	31
17	2	18
18	6	39
19	2	20
20	6	42
21	4	32

Notación Si f es una función aritmética, y n es un entero positivo, entonces el símbolo

$$\sum_{d/n} f(d)$$

indica la suma de todos los términos $f(d)$, donde d es un divisor de n.

Teorema 3.3.1 *Sea f una función multiplicativa y*

$$F(n) = \sum_{d/n} f(d)$$

entonces F es multiplicativa.

Demostración:

Sean m y n enteros positivos tales que $(m, n) = 1$. Debemos demostrar entonces $F(mn) = F(n)F(m)$, para lo cual supondremos que m y n tienen descomposición en factores primos de la forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \quad , \quad m = q_1^{\delta_1} q_2^{\delta_2} \cdots q_t^{\delta_t}.$$

Entonces los divisores de mn son todos de la forma

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s} q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_t^{\lambda_t},$$

donde $0 \leq \gamma_i \leq \alpha_i$, $0 \leq \lambda_j \leq \beta_j$.

Por lo tanto

$$\begin{aligned} F(m,n) &= \sum_{d/mn} f(d) \\ &= \sum_{0\leq\gamma_i\leq\alpha_i\leq \ 0\leq\lambda_j\leq\beta_j} f(p_1^{\gamma_1}\cdots p_s^{\gamma_s} q_1^{\lambda_1}\cdots q_t^{\lambda_t}) \\ &= \sum_{0\leq\gamma_i\leq\alpha_i} \ \sum_{0\leq\lambda_j\leq\beta_j} f(p_1^{\gamma_1}\cdots p_s^{\gamma_s)} f(q_1^{\lambda_1}\cdots q_t^{\lambda_t}) \\ &= \sum_{d_1/n} \sum_{d_2/m} f(d_1) f(d_2) \\ &= \left(\sum_{d_1/n} f(d_1)\right)\left(\sum_{d_2/m} f(d_2)\right) \\ &= F(n)F(m). \end{aligned}$$

♠

Teorema 3.3.2 *La función $d(n)$= número de divisores de n, es multiplicativa.*

Demostración:

Usamos el resultado anterior, haciendo $f(n) = 1$. Luego

$$d(n) = \sum_{d/n} 1$$

es multiplicativa. ♠

Teorema 3.3.3 *La función $\sigma(n)$= suma de los divisores de n, es multiplicativa.*

Demostración:

Nuevamente, por intermedio del teorema 3.3.2 se obtendrá el resultado. Tomando $f(n) = n$, nos produce:

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

Claramente σ es multiplicativa en virtud del teorema 3.3.2. ♠

Una vez que hemos demostrado este par de teoremas, nos resulta relativamente fácil calcular los valores de las funciones $d(n)$ y $\sigma(n)$ cuando se conoce la descomposición prima de n. Unicamente falta obtener fórmulas para estas funciones en el caso de ser n una potencia de un primo, lo cual no es muy difícil; como se verá a continuación.

Si p es primo, entonces los divisores de una potencia de p, digamos p^α, son $1, p, p^2, \cdots p^{\alpha-1}, p^\alpha$. Luego se tiene

$$d(p^\alpha) = \alpha + 1,$$

y

$$\begin{aligned} \sigma(p^\alpha) &= 1 + p + \cdots + p^\alpha \\ &= \frac{1 - p^{\alpha+1}}{1 - p^\alpha}. \end{aligned}$$

Podemos resumir todas estas observaciones en el siguiente corolario.

Corolario 3.3.1 *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, con p_i primos, se tiene:*

$$\begin{aligned} &a) \quad d(p) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1) \\ &b) \quad \sigma(n) = \left(\frac{1 - p_1^{\alpha_1+1}}{1 - p_1^{\alpha_1}}\right) \cdots \left(\frac{1 - p_s^{s+1}}{1 - p_s^{\alpha_s}}\right) \end{aligned}$$

Ejercicios

1) Construir una tabla con los valores de n, $1 \leq n \leq 100$ para las funciones
a) $\varphi(n)$
b) $d(n)$
c) $\sigma(n)$.

2) Hallar un sistema reducido de residuos módulo 25.

3) Sea n un entero positivo fijo. Demostrar que la ecuación $\varphi(x) = n$ posee un número finito de soluciones.

4) Hallar el menor entero x para el cual $\sigma(2x) = 2\varphi(x)$.

5) **Números perfectos:** un entero positivo n se dice perfecto si n es igual a la suma de sus divisores, diferentes de n (divisores propios). Por ejemplo: $6 = 3+2+1$ = suma de sus divisores propios.

Pregunta: ¿Existen números perfectos? La respuesta es sí, 28 y 496 también son perfectos (verficarlo!).

Pregunta: ¿Existen infinitos números perfectos? No se sabe hasta el presente.

Probar:
a) n es perfecto, si y sólo si $\sigma(n) = 2n$.
b) Usando el resultado anterior, probar lo siguiente: si $2^\alpha - 1$ es primo, entonces $2^{\alpha-1}(2^\alpha - 1)$ es perfecto.

6) **Primos de Mersene:** Un número primo de la forma $2^\alpha - 1$, se llama un primo de Mersene, por ejemplo: $3 = 2^2 - 1$, $31 = 2^5 - 1$.

Pregunta: ¿Existen infinitos primos de Mersene? No se conoce la respuesta. Se sabe que $2^{19937} - 1$ es un primo de Mersene que contiene 6002 dígitos!. Hallar otro primo de Mersene distinto de los dados como ejemplos.

7) **Función de Mobius:** Considerese la función aritmética

$$\mu(n) = \begin{cases} 1, & \text{si} \quad n = 1 \\ 0, & \text{si} \quad n \text{ es divisible por un cuadrado } d \neq 1 \\ (-1)^r, & \text{si} \quad n = p_1 p_2 \cdots p_r,\ p_i \text{ primos diferentes.} \end{cases}$$

a) Probar que μ es multiplicativa
b) Probar

$$\sum_{d/n} \mu(d) = 0, \quad \text{si } n > 1$$

8) Halle un sistema reducido de residuos módulo 10 en el conjunto $\{11, 12, \ldots, 20\}$

9) Calcular $\mu(429)$, $\mu(400)$ y $\mu(505)$.

10) Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, donde los p_i son primos distintos. Probar la fórmula:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right)$$

3.4 Teoremas de Euler y Fermat

En esta sección, m será un número entero positivo mayor que 1.

Teorema 3.4.1 *Sea $x_1, \cdots, x_n$ un sistema reducido de residuos módulo m, y sea a un entero tal que $(a, m) = 1$. Luego $ax_1, \cdots, ax_n$ es también un sistema reducido módulo m.*

Demostración:

En primer lugar, debemos probar que los ax_i son incongruentes módulo m. En efecto, supongamos que para algunos i, j se tiene

$$ax_i \equiv ax_j \, mod \, m.$$

Esto implica que m divide a $(ax_i - ax_j)$ y de esto se deduce $m|x_i - x_j$, pues $(a, m) = 1$ por hipótesis. Por lo tanto se tiene que

$$x_i \equiv x_j \ mod \ m,$$

con lo cual $x_i = x_j$, porque los x_i son incongruentes entre sí. Con esto queda probada la primera parte de la demostración.

En segundo lugar, es claro que para todo i se tiene que $(ax_i, m) = 1$, pues $(x_i, m) = 1$ y además $(a, m) = 1$. Es decir, x_i y a no poseen factores primos comunes con m y en consecuencia ax_i tampoco tiene factores en común con m.

Por último, resta probar que si c es un entero con $(c, m) = 1$, entonces existe un i tal que

$$ax_i \equiv c \ mod \ m.$$

Notemos que la ecuación lineal de congruencia

$$ax \equiv c \ mod \ m \tag{3.1}$$

siempre se puede resolver, con las hipótesis que tenemos sobre a, c y m. Por lo tanto, sea y_0 una solución de (3.1), la cual debe cumplir

$$ay_0 = c + mt,$$

para algún t entero. Si m divide a y_0, entonces m divide a c, lo cual es imposible. Por lo tanto debe ser $(y_0, m) = 1$, con lo cual obtenemos

$$y_0 \equiv x_i \ mod \ m,$$

para algún i, y de aquí se deduce:

$$ay_0 \equiv ax_i \ mod \ m.$$

Sustituyendo este resultado en la ecuación (3.1) nos da:

$$c \equiv ay_0 \equiv ax_i \ mod \ m,$$

y con esto termina la demostración. ♠

Teorema 3.4.2 *(Teorema de Euler) Si a es un entero, con $(a, m) = 1$, entonces se tiene*

$$a^{\varphi(m)} \equiv 1 \ mod \ m.$$

Demostración:

Sea $x_1, \cdots, x_n$ un sistema reducido de residuos módulo m, luego $n = \varphi(m)$. En virtud del teorema anterior: $ax_1, \cdots, ax_n$ es también un sistema reducido, y en particular obtenemos que para todo i existe un j tal que

$$x_i \equiv ax_j \ mod \ m \tag{3.2}$$

donde $1 \leq i \leq n$, $1 \leq j \leq n$.

En realidad, para cada i se tiene una ecuación del tipo (3.2). Luego multiplicando $x_1 x_2 \cdots x_n$ y usando las ecuaciones dadas para cada x_i, obtenemos

$$\prod_{i=1}^{n} x_i \equiv a^n \prod_{j=1}^{n} x_j \, mod \, m \tag{3.3}$$

Observemos que cada uno de los términos x_i es primo relativo con m, luego el producto de todos ellos también lo es, y en consecuencia podemos dividir ambos miembros de (3.3) entre este producto, para obtener

$$a^n \equiv a^{\varphi(m)} \equiv 1 \ mod \ m.$$

Con lo cual se da fin a la prueba. ♠

Teorema 3.4.3 *(Teorema de Fermat) Si p es primo, entonces*

$$a^{p-1} \equiv 1 \ mod \ p$$

Demostración:

Notemos que la condición $p|a$ implica $(a, p) = 1$, y de acuerdo al teorema anterior se debe tener

$$a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \ mod \ p$$

♠

El teorema de Euler posee el siguiente corolario, muy importante:

Corolario 3.4.1 *Sean a y b dos enteros, con $(a, m) = 1$. Entonces la ecuación lineal de congruencia*

$$ax \equiv b \; mod \; m \tag{3.4}$$

posee solución

$$x \equiv a^{\varphi(m)-1} b \; mod \; m$$

Demostración:

De acuerdo al teorema 3.4.3 se tiene que $a^{\varphi(m)} \equiv 1 \; mod \; m$. Luego multiplicando (3.4) por $a^{\varphi(m)-1}$ se obtiene el resultado deseado. ♠

Ejemplo 6:

Resolver la congruencia

$$3x \equiv 2 \; mod \; 5$$

Solución: Usando el teorema anterior se tiene:

$$\begin{aligned} x &\equiv 3^{\varphi(5)-1} 2 \, mod \, 5 \\ &\equiv 3^3 2 \, mod \, 5 \\ &\equiv 54 \, mod \, 5 \end{aligned}$$

Luego $x \equiv 4 \; mod \; 5$.

Observación 1: El teorema de Fermat se puede generalizar a cualquier grupo de manera siguiente:

Si G es un grupo de n elementos, entonces para todo elemento $a \in G$ se tiene

$$a^n = e,$$

donde e es el elemento neutro de G.

Observación 2: En el capítulo 2, sección 4, vimos que si p es primo, entonces el conjunto de enteros módulo p, denotado por $\mathbb{Z}_p$, es un cuerpo. Por lo tanto, todo elemento distinto de cero en $\mathbb{Z}_p$ posee un inverso multiplicativo.

Por ejemplo si $p = 7$ en $\mathbb{Z}_7$ tenemos

$$2 \cdot 4 \equiv 1 \ mod\ 7 \quad ; \quad 3 \cdot 5 \equiv 1 \ mod\ 7 \quad ; \quad 6 \cdot 6 \equiv 1 \ mod\ 7$$

Luego se tiene

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 &\equiv 6 \, mod\, 7 \\ 6! &\equiv -1 \, mod\, 7 \end{aligned}$$

Teorema 3.4.4 *(Teorema de Wilson)*

$$p \text{ es primo} \iff (p-1)! \equiv -1 \ mod\ p$$

Demostración:

Si $p = 2$ el resultado es evidente. Supongamos que $p > 2$

Sea $A = \{1, 2, \cdots, p-1\}$. De acuerdo a la observación anterior, cada elemento x en A, posee un inverso multiplicativo en A. En otras palabras, para cada x, $1 \leq x \leq p-1$, existe un y, $1 \leq y \leq p-1$, tal que

$$xy \equiv 1 \ mod\ p$$

Posiblemente suceda que $x = y$, en algunos casos, pero veamos cuando puede ocurrir esto. Si $x^2 \equiv 1 \ mod\ p$, entonces p divide a $(x+1)(x-1)$, y como p es primo se tendrá:

i) $p|x+1$, y en este caso

$$x \equiv -1 \equiv p-1 \ mod\ p,$$

o bien

ii) $p|x-1$, y en este caso se tiene

$$x \equiv 1 \ mod \ p.$$

Así pues, los únicos elementos de A que satisfacen la condición $x^{-1} = x$ son $x = 1$ y $x = p-1$. Por lo tanto cada x de A, distinto de 1 y $p-1$, se puede agrupar con su inverso $y \neq x$, y al multiplicar ambos obtenemos uno. Si multiplicamos ahora todos los elementos de A, y los agrupamos en pares (x, y) donde y es el inverso de x, obtendremos $(p-3)/2$ parejas de la forma (x, y) con $xy = 1$, lo cual produce $(p-3)/2$ unos, y por lo tanto

$$\begin{aligned} (p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) &\equiv \overbrace{1 \cdot 1 \cdot 1 \cdots 1}^{(p-3)/2 \text{ veces}}(p-1) \, mod \, p \\ &\equiv p-1 \, mod \, p \\ &\equiv -1 \, mod \, p \end{aligned}$$

Recíprocamente, si

$$(p-1)! \equiv -1 \ mod \ p,$$

entonces de esta congruencia se deduce lo siguiente: ningún x, con $1 \leq x \leq p-1$ divide a p, luego p es primo.

♠

Ejercicios

1) Verifique el teorema de Euler para $m = 7$ y a tomando los valores $2, 3, 4, 5$ y 6.

2) Verifique el teorema de Fermat para $p = 11$ y $a = 3$.

3) Hállese el mínimo valor de n para el cual $5^n \equiv 1 \ mod \ 7$.

4) Si p es primo, impar y $x \equiv -1 \ mod \ p$, demuéstrese que

$$x^{p-2} + x^{p+3} + \cdots + x + 1 \equiv 0 \ mod \ p$$

5) Resolver la congruencia: $6x \equiv 2 \ mod \ 7$.

6) Resolver $x^{80} \equiv 2 \ mod \ 5$.

7) En $\mathbb{Z}_{11}$, hallar los inversos multiplicativos de 3,5 y 9.

8) ¿Es $2^{100} - 1$ un número primo?.

9) Demuestre que 35 divide a $6^{24} - 1$. *Ayuda* : $\varphi(35) = 24$.

10) Demuestre que $(p-1)! \equiv -1 \ mod \ p$, entonces p es primo.

11) Demuestre que si $p \equiv 1 \ mod \ 4$ entonces la congruencia

$$x^2 \equiv -1 \ mod \ p$$

posee solución.

12) Hallar las soluciones de
a) $x^2 \equiv -1 \ mod \ 13$,
b) $x^2 \equiv -1 \ mod \ 17$

13) Demuestre que si $p \equiv 1 \ mod \ 4$, se puede resolver

$$x^2 + y^2 \equiv 0 \ mod \ p$$

14) Hallar una solución de $x^2 + y^2 \equiv 0 \ mod \ 13$.

15) Probar que $x^5 - x$ es divisible por 5,8 y 10, para todo entero x.

16) Probar que $x^{16} - x$ es divisible por 32, para todo x entero.

17) Si p es primo, hallar el inverso multiplicativo de $(p-1)!$ en $\mathbb{Z}_p$.

18) Hallar las soluciones de
a) $15x \equiv 2 \ mod \ 17$,
b) $8x \equiv 3 \ mod \ 15$.

19) En $\mathbb{Z}_{11}$, hallar todos los elementos y tales que $y = x^2$ para algún x en $\mathbb{Z}_{11}$.

20) Hallar todas las soluciones de $x^3 \equiv 1 \ mod \ 11$.

21) Verificar el teorema de Fermat para el grupo de los enteros módulo m con la adición.

22) Construir un ejemplo de un grupo finito de 6 elementos, y verifíquese el teorema de Fermat, en el mismo.

3.5 Congruencias Polinomiales

En el capítulo 2, vimos como se resolvía una congruencia lineal

$$ax \equiv b \; mod \; m$$

en donde a y b son enteros.

En esta sección y las siguientes, nos ocuparemos de resolver congruencias del tipo

$$f(x) \equiv 0 \; mod \; m, \tag{3.5}$$

donde $f(x)$ es un polinomio con coeficientes enteros. Es decir

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

con a_i entero, $1 \leq i \leq n$.

Notemos que x_1 es solución de (3.5), entonces todo entero b que satisface $b \equiv x_1 \; mod \; m$, también es solución (verificarlo!), luego consideramos solo aquellas soluciones distintas módulo m.

Observación: La teoría de polinomios módulo m, difiere un poco de la teoría general de polinomios sobre $\mathbb{Q}$.

Sabemos que en $\mathbb{Q}[x]$ todo polinomio de grado n, posee a lo sumo n raíces. Esto es falso en general para polinomios módulo m. Por ejemplo el polinomio de grado 2 en los enteros módulo 6,

$$f(x) = x^2 - x$$

tiene 4 raíces las cuales son 0,1,3 y 4.

En el ejemplo 9 se estudia el polinomio

$$x^3 - 2x^2 - 9 \, mod \, 125,$$

el cual tiene 11 raíces.

Sin embargo si p es un número primo, veremos que todo polinomio sobre $\mathbb{Z}_p$ de grado n, posee a lo sumo n raíces.

Existe una relación importante entre los polinomios en $\mathbb{Z}[X]$ y polinomios en $\mathbb{Z}_m[x]$.

Teorema 3.5.1 *Sea $f(x)$ un polinomio con coeficientes enteros, Si $f(x)$ es irreducible módulo m para algún m, entonces $f(x)$ es irreducibles en $\mathbb{Z}[x]$.*

Ejemplo: El polinomio $f(x) = x^2 + 1$, es irreducible en $\mathbb{Z}_3$. Luego $f(x)$ es irreducible en $\mathbb{Z}[x]$ y por lo tanto en $\mathbb{Q}[x]$, pues $f(x)$ es mónico.

En lo sucesivo y hasta el resto de este capítulo, todos los polinomios considerados, son de coeficientes enteros.

A fin de simplificar los cálculos en las congruencias polinomiales, introduciremos la siguiente definición.

Definición 3.5.1 *Dos polinomios f y g de grados m y n, con $m \geq n$*

$$f(x) = a_m x^m + \cdots + a_1 x + a_0$$
$$g(x) = b_n x^n + \cdots + b_1 x + b_0$$

se dicen **congruentes módulo** m **polinomio**, *y lo denotamos por*

$$f(x) \equiv_x g(x) \, mod \, m$$

Si $a_i \equiv 0 \; mod \; m$, para $i > n$, y $a_i \equiv b_i \; mod \; m$, y para todo i, $1 \leq i \leq n$.

Ejemplo 7:

$$10x^{13} + 17x^2 + 25x - 6 \equiv_x 2x^2 - 1 \, mod \; 5$$

Vemos con este ejemplo, la importancia de la definición anterior en lo que respecta a la simplificación de las operaciones. Es evidente que el polinomio de la derecha es mucho fácil de manipular que el de la izquierda.

Observación: Si $f(x)$ es un polinomio, entonces la congruencia normal

$$f(x) \equiv 0 \; mod \; p$$

no implica necesariamente que

$$f(x) \equiv_x 0 \, mod \, p.$$

Por ejemplo, si p es un número primo, entonces por el teorema de Fermat se tiene

$$x^p - x \equiv 0 \; mod \; p$$

para todo x entero.

Luego el polinomio $f(x) = x^p - x$ es congruente módulo p al polinomio 0. Si embargo $f(x)$ no es congruente a 0 módulo polinomio, pues los coeficientes de $f(x)$ no son congruentes módulo p a los coeficientes del polinomio 0.

El primer paso que daremos en la resolución de una ecuación del tipo (3.5), será reducir el tamaño del módulo, el cual puede ser un número muy grande. Supongamos que m se factoriza

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

entonces usando el mismo razonamiento empleado en las ecuaciones lineales en el capítulo 2, se tiene el siguiente resultado:

Teorema 3.5.2 *Sea f un polinomio. Entonces toda solución de*

$$f(x) \equiv 0 \; mod \; m \tag{3.6}$$

es solución del sistema

$$\begin{aligned} f(x) &\equiv 0 \; mod \; p_1^{\alpha_1} \\ f(x) &\equiv 0 \; mod \; p_2^{\alpha_1} \\ &\cdots \\ f(x) &\equiv 0 \; mod \; p_s^{\alpha_s} \end{aligned} \tag{3.7}$$

Recíprocamente, toda solución del sistema (3.7) es solución de (3.6).

De acuerdo a este teorema, el problema de resolver congruencias polinomiales, módulo un número compuesto se reduce a resolver congruencias polinomiales módulo potencias de primos.

Ejemplo 8:

Resolver:

$$2x^2 + x - 1 \equiv 0 \, mod \, 20$$

Solución:

De acuerdo al teorema anterior, esta ecuación es equivalente al sistema

$$\begin{aligned} 2x^2 + x - 1 &\equiv 0 \ mod \ 4 \\ 2x^2 + x - 1 &\equiv 0 \ mod \ 5. \end{aligned}$$

Por inspección directa, vemos que las soluciones módulo 20 de la primera y segunda ecuación, son respectivamente:

$$x = 3, 7, 11, 15, 19 \quad \text{y} \quad y = 4, 9, 14, 19$$

Luego la solución de la ecuación original (módulo 20), será la solución común a ambos sistemas, es decir, $x \equiv 19 \ mod \ 20$

Seguidamente, haremos un estudio de la congruencia

$$f(x) \equiv 0 \ mod \ p^{\alpha} \tag{3.8}$$

donde p es primo. Probaremos que esta ecuación se puede resolver cuando se conoce la solución de

$$f(x) \equiv 0 \ mod \ p \tag{3.9}$$

Antes de entrar de lleno en la demostración de esto, necesitamos algunas herramientas del álgebra de polinomios. Supondremos que el lector conoce el concepto de derivada de orden i de una función la cual denotaremos por $f'(x)$.

Teorema 3.5.3 *Sean x e y y números enteros, y f un polinomio de grado n, entonces*

$$f(x+y) = f(x) + \frac{f'(x)}{1!}y + \frac{f''(x)}{2!}y^2 + \cdots + \frac{f^n(x)}{n!}y^n$$

y además los coeficientes $\dfrac{f^i(x)}{i!}$ son todos enteros, $1 \leq i \leq n$.

Demostración:

Observamos en primer lugar que el grado de f es n, y por lo tanto todas las derivadas de órdenes superiores a n, son nulas, y en consecuencia la serie de Taylor es finita. En particular el resto de orden $n+1$ es cero, luego la fórmula anterior es correcta. Solo falta probar que los términos $f^i(x)/i!$ son todos enteros, lo cual probaremos en el caso de ser $f(x) = ax^k$ un monomio (¿Por qué ?).

Luego tenemos

$$\frac{f^i(x)}{i!} = \frac{ak(k-1)(k-2)\cdots(k-i+1)}{1\cdot 2\cdot 3\cdots i}x^{k-i}, \qquad 1 \leq i \leq k.$$

Nótese que

$$\left(\begin{array}{c} k \\ i \end{array}\right) = \frac{k!}{(k-i)!i!} = \frac{k(k-1)\cdots(k-i-1)}{1\cdot 2\cdots i}$$

es un entero, y por lo tanto

$$\frac{f'(x)}{i!} = a\left(\begin{array}{c} k \\ i \end{array}\right)x^{k-i}$$

es también un número entero. ♠

Consideremos ahora el par de congruencias

$$f(x) \equiv 0 \ mod\ p^{\alpha+1} \tag{3.10}$$
$$f(x) \equiv 0 \ mod\ p^{\alpha} \tag{3.11}$$

Sea a una solución de (3.10), entonces necesariamente se sigue que a es solución de (3.11). Luego podemos hacer $a = b + kp^{\alpha}$, donde b es una solución de (3.11), y k es un entero a determinar. Veremos a continuación, que es posible obtener todas las soluciones de (3.10) a partir de las soluciones de (3.11), en la forma indicada, imponiendo ciertas condiciones sobre el entero k.

Teorema 3.5.4 *Sea b solución de (3.11), entonces $b + kp^{\alpha}$ es solución de (3.10), si y sólo si*

$$kf'(b) \equiv -\frac{f(b)}{p^{\alpha}} \, mod \, p \tag{3.12}$$

Demostración:

Usando la fórmula de Taylor tenemos

$$f(b + kp^{\alpha}) = f(b) + \frac{f'(b)kp^{\alpha}}{1} + \cdots \frac{f^{n}(b)(kp^{\alpha})^{n}}{n!}$$

Nótese que los términos

$$\frac{f'(b)}{1}, \frac{f''(b)}{2!}, \cdots, \frac{f^{n}(b)}{n!}$$

son todos enteros, y por lo tanto los términos del lado derecho en la serie de Taylor, son todos enteros. Luego

$$f(b + kp^{\alpha}) \equiv f(b) + f'(b)kp^{\alpha} \, mod \, p^{\alpha+1}$$

Si $b + kp^{\alpha}$ es solución de (3.10), se tendrá:

$$f(b + kp^{\alpha}) \equiv 0 \, mod \, p^{\alpha+1},$$

y por consiguiente

$$f'(b)kp^{\alpha} \equiv f(b) \, mod \, p^{\alpha+1} \tag{3.13}$$

Como b es solución de (3.11) se tiene que:

$$f(b) \equiv 0 \ mod \ p^{\alpha}$$

luego p^{α} divide a $f(b)$ y por lo tanto podemos dividir la ecuación de congruencia (3.13) entre p^{α} para obtener

$$f'(b)k \equiv \frac{f(b)}{p^{\alpha}} \, mod \, p$$

con lo cual queda probado el teorema ♠

A continuación, haremos un estudio detallado de la ecuación de congruencia (3.12), en donde analizaremos los posibles valores de $f'(b)$ módulo p

Teorema 3.5.5 *Sean $a = b + kp^{\alpha}$, como en el teorema 3.5.4. Entonces se presentan dos casos:*

i) Si $f'(b) \equiv 0 \, mod \, p$, a es solución de (3.10) si y sólo si b es solución de (3.11) (no hay restricción sobre k).

ii) Si $f'(b) \not\equiv 0 \ mod \ p$, existe un único valor k para el cual a es solución de (3.10).

Demostración:

Caso I): Si $f'(b) \equiv 0 \ mod \ p$, entonces (3.12) se puede resolver si y sólo si $f(b) \equiv 0 \, mod \, p^{\alpha+1}$, lo cual implica que b es solución de (3.10). El recíproco también es cierto.

Caso II): Si $f'(b) \not\equiv 0 \ mod \ p$ se tiene $(f'(p), p) = 1$ y por lo tanto, $f'(p)$ tiene un inverso bajo el producto módulo p. Sea t este inverso y multipliquemos la ecuación (3.12) por t para obtener

$$k \equiv -\frac{tf(b)}{p^{\alpha}} \, mod \, p.$$

Al evaluar $f(b)$ no debe hacerse la reducción módulo p.

Luego existe un único valor de k módulo p, que hace a a solución de (3.10). ♠

Ejemplo 9:

Resolver:

$$f(x) = x^3 - 2x^2 - 9 \equiv 0 \, mod \, 125 \tag{3.14}$$

Solución:

En primer lugar resolvemos.

$$f(x) = x^3 - 2x^2 - 9 \equiv 0 \; mod \; 5$$

esto es

$$x^3 - 2x^2 + 1 \equiv 0 \; mod \; 5. \tag{3.15}$$

Podemos hallar una solución, si existe, por intermedio de la tabla siguiente:

tabla módulo 5

x	x^2	x^3	$x^3 - 2x^2 + 1$
0	0	0	1
1	1	1	0
2	4	3	1
3	4	2	0
4	1	4	3

Luego las soluciones son $x \equiv 1, 3 \; mod \; 5$
Tomemos $x = 1$ y consideremos aquellas soluciones del tipo

$$a = 1 + 5k \tag{3.16}$$

y veamos cuál de éstos es solución de

$$x^3 - 2x^2 - 9 \equiv 0 \; mod \; 25 \tag{3.17}$$

Para tal fin, calculamos las cantidades involucradas en el teorema anterior

$$f'(x) = 3x^2 - 4x$$

luego

$$f'(1) = 3 - 4 \equiv -1 \equiv 4 \, mod \, 5$$

luego despejamos k de la ecuación

$$f'(1)k \equiv \frac{-f(1)}{p} \, mod \, p,$$

teniendo cuidado que $f(1)$ se calcula de acuerdo (3.14) sin hacer la reducción módulo 5.

Así pues, tenemos

$$4k \equiv \frac{+10}{5} \, mod \, 5$$

o sea

$$4k \equiv +2 \; mod \; 5$$

de donde

$$k = 3.$$

Sustituyendo en (3.16) tenemos que

$$a = 1 + 3 \cdot 5 = 16$$

es la única solución de (3.17) proveniente de $x = 1$.

Repetimos el mismo argumento para la ecuación (3.17), haciendo ahora

$$a = 16 + 25 \cdot k. \tag{3.18}$$

donde k es un nuevo valor a determinar

Nótese que

$$f'(16) = 3(16)^2 - 4(16) = 704 \equiv 4 \, mod \, 5$$

Luego despejamos el valor de k en la ecuación

$$f'(16)k \equiv \frac{-f(16)}{p^2} \, mod \, p,$$

de donde

$$\begin{aligned} 4 \cdot k &\equiv \frac{-3575}{25} \, mod \, 5 \\ &\equiv -143 \, mod \, 5 \\ &\equiv -3 \, mod \, 5 \\ &\equiv 2 \, mod \, 5 \end{aligned}$$

de donde

$$k = 3.$$

Luego

$$a = 16 + 25 \cdot 3 = 91$$

es una solución de (3.14).

Veamos qué sucede si volvemos hacia atrás y tomamos $x = 3$ como solución de (3.15).

Consideremos soluciones del tipo

$$a = 3 + 5 \cdot k$$

Para determinar el valor de k admisible, en la ecuación (3.17) usamos el teorema

$$f'(3) = 3(3)^2 - 4(3) \equiv 15 \equiv 0 \, mod \, 5.$$

Además

$$f(3) = 0 \equiv 0 \, mod \, 25$$

y por lo tanto todos los valores de k son admisibles. Así pues tenemos: x = 3,8,13,18 y 23 soluciones de (3.17).

Podemos repetir el proceso para cada uno de estos valores. Esto se expresa en la siguiente

tabla módulo 5

x	$f(x)$	$f'(x)$	$f(x) \, mod \, 125$	$f'(x) \, mod \, 5$
3	0	15	0	0
8	375	160	0	0
13	1850	455	60	0
18	5175	900	50	0
23	11100	1495	100	0

De acuerdo a la tabla se tiene que $x = 3$ y $x = 8$ aportan nuevas soluciones. Los valores restantes de x: 13, 18 y 23 no generan solución alguna.

Luego

$$3 + 25 \cdot k$$

es solución de (3.14) para todo $k = 0, 1, 2, 3, 4$. Esto genera las 5 soluciones

$$\{3, 28, 53, 78, 103\}$$

Igualmente, se deduce que

$$8 + 25 \cdot k$$

es solución de (3.14) para todo $k = 0, 1, 2, 3, 4$, lo cual genera las soluciones

$$\{8, 33, 58, 83, 108\}$$

Resumiendo entonces, la ecuación (3.14) posee 11 soluciones dadas por

$$\{3, 8, 28, 33, 53, 58, 78, 83, 91, 103, 108\}$$

Ejemplo 10:

Resolver:

$$x^3 - 2x^2 + 2 \equiv 0 \, mod \, 125$$

Solución:

En primer lugar resolvemos

$$x^3 - 2x^2 + 2 \equiv 0 \, mod \, 5$$

Por simple inspección, vemos que no posee solución. Luego la ecuación dada tampoco posee solución.

3.6 Congruencias Módulo Primo

En esta sección se continua con el estudio de las congruencias polinomiales del tipo visto en la sección anterior, pero tomando como módulo un número primo p. Bajo esta condición, se tienen muy buenos resultados, algunos de ellos provenientes del álgebra de los polinomios, como por ejemplo el teorema de Lagrange que establece: Todo polinomio de grado n posee a lo sumo n raíces. Finalmente, haremos un estudio particular de las ecuaciones cuadráticas módulo p.

Teorema 3.6.1 *Sea $f(x)$ un polinomio de grado n, con coeficientes enteros, y sea a un entero cualquiera. Entonces existe un polinomio $q(x)$ con coeficientes enteros, tal que*

$$f(x) = (x-a)q(x) + f(a)$$

y además, grado $(q(x)) = n-1$.

Demostración:

Podemos aplicar la división de polinomios entre $f(x)$ y $x-a$, para obtener

$$f(x) = (x-a)q(x) + r,$$

donde el grado de $r <$grado $(x-a) = 1$.

Por lo tanto grado $r = 0$ y así pues r es una constante, que se puede determinar al sustituir x por a en la ecuación de arriba. Esto nos da

$$f(a) = (a-a)q(a) + r = r.$$

Solo resta probar que q posee coeficientes enteros, lo cual es fácil ver pues en el proceso de división de f entre $x-a$, no es necesario dividir en ningún momento. Para reafirmar lo dicho $q(x)$ se expresa por

$$q(x) = a_n x^{n-1} + (a_{n-1} + aa_n)x^{n-2} + \cdots + (-a_1 x),$$

si

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Con esto termina la demostración ♠

Ejemplo 11:

Sea

$$f(x) = x^4 - 3x^3 + 2x^2 + 5$$

y $a = 1$.

Luego $f(1) = 5$ y así pues, se tiene

$$f(x) = (x-1)q(x) + 5$$

donde $q(x)$ es el polinomio de grado 3: $q(x) = x^3 - 2x^2$.

Teorema 3.6.2 *(Teorema de Lagrange) Sea p un número primo y sea f un polinomio de grado n $(n \leq p)$ con coeficientes enteros. Entonces la congruencia*

$$f(x) \equiv 0 \, mod \, p \tag{3.19}$$

posee a lo sumo n soluciones distintas.

Demostración:

Sean $r_1, \cdots, r_s$ soluciones distintas módulo p de (3.19). Entonces $f(r_i) \equiv 0 \, mod \, p$, $1 \leq i \leq s$. Por el teorema 3.6.1 existe un polinomio $q_1(x)$ de grado menor n tal que

$$f(x) \equiv (x - r_1)q_1(x) \ mod \ p \tag{3.20}$$

Tomando $x = r_2$ en (3.20) obtenemos

$$0 \equiv f(r_2) \equiv (r_2 - r_1)q_1(r_2) \, mod \, p,$$

y por lo tanto p divide a $(r_2 - r_1)q_1(r_2)$. Como p es primo se tiene que

$$r_2 - r_1 \equiv 0 \, mod \, p, \quad \text{ó} \quad q_1(r_2) \equiv 0 \, mod \, p.$$

Lo primero no puede ocurrir, pues por hipótesis las soluciones r_1, $r_2, \cdots, r_s$ son distintas módulo p y por lo tanto se obtiene

$$q_1(r_2) \equiv 0 \, mod \, p.$$

Por un razonamiento análogo al anterior, se deduce que las restantes $s - 1$ soluciones de (3.19), $r_2, r_3, \cdots r_s$ satisfacen la ecuación

$$q_1(x) \equiv \ 0 \, mod \, p.$$

Como el grado de $q_1(x)$ es menor que n, podemos usar inducción sobre n, para afirmar que $q_1(x)$ posee a lo sumo $n - 1$ raíces.

Luego el conjunto $\{r_2, r_3, \cdots, r_s\}$ posee a lo sumo $n-1$ elementos. Es decir, $s-1 \leq n-1$, lo cual implica que $s \leq n$. ♠

Ejemplo 12:

Resolver la congruencia:

$$12x^{17} + 68x^8 + 393 \equiv 0 \, mod \, 7 \tag{3.21}$$

Solución:

En primer lugar podemos reducir los coeficientes del polinomio dado. Esto es:

$$12x^{17} + 68^8 + 393 \equiv_x 5x^{17} + 5x^8 + 1 \, mod \, 7$$

Luego la ecuación original (3.21) se transforma en

$$5x^{17} + 5x^8 + 1 \equiv 0 \, mod \, 7 \tag{3.22}$$

Observamos que en la ecuación anterior, algunas potencias de x son de grado superior a 7. Es posible simplificar esto también, mediante la utilización del teorema de Fermat, el cual establece:

$$x^6 \equiv 1 \; mod \; 7 \tag{3.23}$$

para todo x.

Usando la ecuación anterior, se puede reducir las potencias de x, de grado mayor que 7. Por ejemplo

$$\begin{gathered} x^7 \equiv x \; mod \; 7 \\ x^8 \equiv x^2 \; mod \; 7 \\ \cdots \\ x^{6k+t} \equiv x^t \, mod \, 7 \end{gathered}$$

para todo entero k, y $1 \leq t \leq 5$.

Luego, (3.22) se transforma en

$$5x^5 + 5x^2 + 1 \equiv 0 \, mod \, 7 \tag{3.24}$$

Podemos eliminar el coeficiente principal 5, multiplicando por el inverso módulo 7 del mismo, el cual es igual 3 (verificarlo!). Haciendo esto nos queda la siguiente ecuación, la cual no admite más simplificación

$$x^5 + x^2 + 3 \equiv 0 \, mod \, 7 \tag{3.25}$$

Por inspección directa, vemos que la única solución es $x = 4$.

3.7 Ecuación Cuadrática

Finalmente, concluimos este capítulo con un estudio detallado de la ecuación polinomial cuadrática módulo un primo p, es decir una ecuación del tipo

$$ax^2 + bx + c \equiv 0 \, mod \, p \tag{3.26}$$

Recordemos que en el caso de las ecuaciones cuadráticas sobre el cuerpo de los números reales se tenía una fórmula explícita para x:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{3.27}$$

En el cuerpo de los enteros módulo p, podemos hacer muchas operaciones similares a las efectuadas en los números reales, aunque desafortunadamente existen algunas limitaciones. En primer lugar no hemos hablado de "extraer raíces cuadradas módulo p". En segundo lugar si $p = 2$ entonces

$$2a \equiv 0 \; mod \; 2$$

y por lo tanto la fórmula anterior carece de sentido en esta situación.

Podemos solventar este y otros inconvenientes con los elementos que tenemos en nuestras manos, sin necesidad de crear nuevos entes matemáticos.

Se puede tratar el caso $p = 2$ como un caso especial, dentro de la teoría que vamos a desarrollar.

La ecuación

$$ax^2 + bx + c \equiv 0 \, mod \, 2$$

se reduce a uno de los cuatros casos

$$\begin{aligned} x^2 &\equiv 0 \ mod \ 2 \\ x^2 + 1 &\equiv 0 \ mod \ 2 \\ x^2 + x &\equiv 0 \ mod \ 2 \\ x^2 + x + 1 &\equiv 0 \ mod \ 2 \end{aligned}$$

y cada uno de estos casos se pueden resolver por tanteo.

De ahora en adelante, supondremos que p es un primo distinto de 2.

En primer lugar, asumiremos que en la ecuación (3.26) el coeficiente a es primo relativo con p (caso contrario se tendría una ecuación lineal, la cual fue estudiada en el capítulo 2). Por lo tanto se tiene $4a \not\equiv \ 0 \ mod \ p$, y al multiplicar la ecuación (3.26) por $4a$, nos queda la siguiente ecuación:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \, mod \, p$$

o sea

$$(2ax + b)^2 + 4ac - b^2 \equiv 0 \, mod \, p$$

y por lo tanto

$$(2ax + b)^2 \equiv b^2 - 4ac \, mod \, p.$$

Haciendo el cambio de variables

$$2ax + b = X \tag{3.28}$$
$$b^2 - 4ac = B \tag{3.29}$$

se tendrá

$$X^2 \equiv B \ mod \ p \tag{3.30}$$

Obsérvese que si resolvemos la ecuación anterior (3.30) para X, entonces el valor de x se puede hallar en (3.28), pues $(2a, p) = 1$ y por lo tanto la ecuación lineal

$$2ax \equiv X - b \, mod \, p$$

siempre posee solución.

Hemos probado entonces:

Teorema 3.7.1 *Sea p un número primo, $p \neq 2$ entonces, toda ecuación cuadrática*

$$ax^2 + bx + c \equiv 0 \, mod \, p$$

es equivalente a una del tipo

$$X^2 \equiv b^2 - 4ac \, mod \, p,$$

donde $B \equiv b^2 - 4ac \, mod \, p$

Observación: En el capítulo 4, nos dedicaremos a estudiar en detalle las ecuaciones cuadráticas del tipo $x^2 \equiv b \ mod \ p$ con $(b, p) = 1$, con p un primo. Si esta ecuación posee solución, entonces diremos que b es un resto cuadrático módulo p

Ejemplo 13:

Resolver:

$$3x^2 + 2x - 1 \equiv 0 \, mod \, 7 \tag{3.31}$$

Solución:

En primer lugar, resolvemos

$$X^2 \equiv b^2 - 4ac \, mod \, p$$

esto es

$$\begin{aligned} X^2 &\equiv 4 - 4(3)(-1) \, mod \, 7 \\ X^2 &\equiv 2 \, mod \, 7 \end{aligned} \tag{3.32}$$

A fin de resolver la ecuación anterior, examinamos todos los posibles restos cuadráticos módulo 7, mediante una tabla. Esto nos da las soluciones $X = 3$ y $X = 4$. Resolvemos ahora el cambio de variable

$$2ax + b \equiv X \, mod \, p,$$

para cada valor de X independientemente. Haciendo esto obtenemos

i)$X = 3$

$$6x + 2 \equiv 3 \; mod \; 7,$$

lo cual nos da

$$x \equiv 6 \; mod \; 7$$

ii)$X = 4$

$$6x + 2 \equiv 4 \; mod \; 7,$$

lo que produce

$$x \equiv 5 \; mod \; 7$$

Claramente estas son las soluciones, únicas módulo 7, de la ecuación original (3.31).

Ejercicios

1) Sea $f(x) = 25x^4 + 36^2 - 163x + 2$. Hallar un polinomio $g(x)$ con coeficientes mínimos tal que

$$g(x) \equiv_x f(x) \, mod \, m,$$

para $m = 5, 10$ y 12.

2) Demuestre que $x^7 \equiv x \ mod \ 7$ para todo x, pero sin embargo, no se tiene $x^7 \equiv_x x \, mod \, 7$.

3) Sea $f(x)$ un polinomio de grado n, tal que

$$f(1) \equiv f(2) \equiv \cdots \equiv f(n+1) \equiv 0 \ mod \, p$$

Probar que $f(x) \equiv 0 \ mod \ p$, para todo x.

4) Probar que lo anterior no se cumple, en general, si p no es primo.

5) Resolver las ecuaciones

a)$x^2 + 15x - 6 \equiv 0 \ mod \ 25$

b)$x^2 + 2x - 15 \equiv 0 \ mod \ 8$

c)$x^3 - 7x^2 + 6 \equiv 0 \ mod \ 27$

6) Aplicando el método de división sintética, hallar el cociente y el resto de dividir

$$(x^4 + 5x^3 - 9x + 16)/(x - 6)$$

7) Resolver las congruencias

a)$2x^2 + x - 1 \equiv 0 \ mod \ 13$

b)$x^2 - 3x + 6 \equiv 0 \ mod \ 7$

c)$5x^2 + 2x - 1 \equiv 0 \ mod \ 11$

8) Demostrar que si x_1 es solución de la congruencia

$$a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \ mod \ m \qquad (*)$$

y si b es otro entero, $b \equiv x_1 \ mod \ m$, entonces b es también solución de la congruencia $(*)$.

9) Resuelva las ecuaciones

a)$6x^2 + 3x - 5 \equiv 0 \ mod \ 21$

b)$9x^3 + 14x^2 - 5x \equiv 0 \ mod \ 15$

10) Reducir los siguientes polinomios

a) $27x^4 + 25x^2 - 31x \, mod \, 3$

b) $71x^{113} + 44x^{22} - x - 102 \, mod \, 11$

11) Resolver:

a)$x^3 + 3x^2 + 3x \equiv 0 \ mod \ 7$

b)$x^3 + 3x^2 + 3x \equiv 0 \ mod \ 11$

c)$127x^8 + 6x - 78 \equiv 0 \ mod \ 5$

d)$x^4 + x^3 + x^2 + x + 1 \equiv 0 \ mod \ 5$

12) Probar el teorema 3.5.2 en el caso $m = pq, p$ y q dos primos distintos.

13) Probar que si B es el número de soluciones de la congruencia

$$f(x) \equiv 0 \ mod \ p^\alpha$$

se tiene que $p|B$.

14) Hallar mediante tablas, todos los restos cuadráticos módulo p, para $p = 5, 7, 11$ y 13.

15) Demuestre que en $\mathbb{Z}_p$, el número de restos cuadráticos es igual al número de restos no cuadráticos. Halle una fórmula para calcular el número de restos cuadráticos módulo p.

16) Resuelva:

a)$x^2 + x + 1 \equiv 0 \ mod \ 2$

b)$x^2 + x \equiv 0 \ mod \ 2$

c)$x^2 + 1 \equiv 0 \ mod \ p$

17) Resolver:

$$3x^{16} + 128x^{10} + 640 \equiv 0 \; mod \; 9$$

18) Factorizar $x^5 - x$ en $\mathbb{Z}_5$ *Ayuda* : Usar el teorema de Fermat.

19) Factorizar $x^4 - 3x^2 + 2x - 1$ en $\mathbb{Z}_2$.

20) Demuestre que si $f(x)$ se puede factorizar de la forma $g(x)h(x)$ en $\mathbb{Z}[x]$, entonces admite la misma factorización en $\mathbb{Z}_p[x]$, para todo p primo. Usando lo anterior, probar $x^2 - 25x + 1$ es irreducible. *Ayuda* : Probar el caso $p = 2$

Capítulo

4

Reciprocidad Cuadrática

En este capítulo estudiamos una serie de resultados dirigidos a demostrar la Ley de Reprocidad Cuadrática, la cual fue probada por Gauss en su libro *Disquisitiones Arithmeticae* en 1801. Gauss dio tres pruebas diferentes de este teorema, y desde entonces han aparecido más de 150 demostraciones distintas.

Por intermedio de esta ley, se pueden determinar si existen soluciones o no, de una ecuación cuadrática del tipo:

$$x^2 \equiv a \ mod \ p, \quad (*)$$

donde p es primo y $(a, p) = 1$.

4.1 Símbolo de Legendre

De ahora en adelante, supondremos que p es primo.

Definición 4.1.1 *Diremos que un entero a es un* **resto cuadrático módulo** *p si la ecuación $(*)$ es soluble.*

Con la finalidad de simplificar las demostraciones introducimos el siguiente símbolo.

Definición 4.1.2 *Sea p primo, y sea a entero, con $(a, p) = 1$. Entonces $\left(\frac{a}{p}\right)$, llamado símbolo de Legendre de a sobre p, se define por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{si } a \text{ es un entero cuadrático mod } p \\ -1, & \text{si } a \text{ no es un resto cuadrático mod } p \end{cases}$$

Ejemplo 1: $\left(\frac{2}{7}\right) = 1$, porque $2 \equiv 3^2 \ mod \ 7$.

Ejemplo 2: $\left(\frac{5}{7}\right) = -1$, porque no existe x tal que $5 \equiv x^2 \ mod\ 7$.

Algunas propiedades elementales del símbolo de Legendre, vienen dadas en el siguiente:

Teorema 4.1.1 *Sea p primo y a, b enteros, primos relativos con p. Luego*

i) $\left(\frac{1}{p}\right) = 1$.

ii) $\left(\frac{a^2}{p}\right) = 1$.

iii) Si $a \equiv b \ mod\ p$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Demostración:

Ciertamente *i)* y *ii)* son triviales.
Para probar *iii)* consideremos dos casos:

Caso I: Si $\left(\frac{a}{p}\right) = 1$, entonces existe un x tal que $a \equiv x^2 \ mod\ p$. Por lo tanto

$$b \equiv a \equiv x^2 \ mod\ p,$$

lo que implica

$$\left(\frac{a}{p}\right) = 1.$$

Caso II: Sea $\left(\frac{a}{p}\right) = -1$, y supongamos que $\left(\frac{b}{p}\right) = 1$, entonces repitiendo el mismo argumento del caso anterior se concluía $\left(\frac{a}{p}\right) = 1$, lo cual contradice la hipótesis. Por lo tanto se debe tener $\left(\frac{b}{p}\right) = -1$. ♠

Teorema 4.1.2 *(Criterio de Euler) Sean p primo y a un entero, con $(a,p)=1$. Entonces*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \ mod\ p.$$

Demostración 1:

Sea b uno cualquiera de entre los números $1, 2, \cdots, p-1$ y consideremos la congruencia

$$bx \equiv a \ mod\ p. \tag{4.1}$$

la cual tiene solución, pues $(b,p)=1$.

Si b' es solución de (4.1), diremos que b y b' son asociados.

Si $\left(\frac{a}{p}\right)=1$, entonces existe un b_1 con $1 \leq b_1 \leq p-1$, y tal que

$$b_1^2 \equiv a \ mod\ p.$$

Además

$$(p-b_1)^2 = p^2 - 2pb_1 + b_1^2 \equiv a \ mod\ p.$$

Luego b_1 y $p-b_1$ son dos soluciones de la ecuación

$$x^2 \equiv a \ mod\ p, \tag{4.2}$$

y por el Teorema de Lagrange, sabemos que éstas son las únicas soluciones.

Podemos concluir, entonces que en el conjunto

$$\{1, 2, \cdots, p-1\} - \{b_1, p-b_1\},$$

cada elemento es diferente de su asociado.

Luego se tienen $(p-3)/3$ pares (b, b'), de elementos asociados distintos, tales que $bb' \equiv a \ mod \ p$, junto con los elementos b_1 y $p - b_1$. Estos son todos los elementos de $\{1, 2, \cdots, p-1\}$.

Multiplicando todos estos $p-1$ elementos se tendrá

$$(p-1)! = 1 \cdot 2 \cdots (p-1) \equiv \ a^{(p-3)/2} b_1 (p - b_1) \ mod \ p$$

o sea

$$(p-1)! \equiv -a^{(p-1)/2} \ mod \ p \tag{4.3}$$

Por otro lado, si $\left(\frac{a}{q}\right) = -1$, los elementos $1, 2, \cdots, p-1$ se pueden agrupar en $(p-1)/2$ pares de asociados distintos. Por lo tanto

$$(p-1)! \equiv a^{(p-1)/2} \ mod \ p \tag{4.4}$$

Usando el teorema de Wilson, tenemos

$$-1 \equiv (p-1)! \equiv a^{\frac{p-1}{2}} \ mod \ p$$

o sea

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod \ p$$

♠

Demostración 2:

Caso I) Si $\left(\frac{a}{p}\right) = 1$, entonces existe x tal que

$$a \equiv x^2 \ mod \ p$$

luego

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv x^{2\frac{(p-1)}{2}} \ mod\ p \\ &\equiv x^{p-1} \ mod\ p \\ &\equiv 1 \ mod\ p \end{aligned}$$

Por lo tanto

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod\ p$$

Caso II) Si $\left(\frac{a}{p}\right) = -1$, entonces a no es cuadrado módulo p. Sean $x_1, \cdots x_s$ los cuadrados en $\mathbb{Z}_p$, donde $s = (p-1)/2$, entonces los elementos no nulos de $\mathbb{Z}_p$ son precisamente

$$x_1, \cdots, x_s, ax_1, \cdots, ax_s$$

por lo tanto

$$x_1 \cdots x_s a x_1 \cdots a x_s \equiv -1 \, mod\, p$$

por el teorema de Wilson.

Pero si x_i es cuadrado, su inverso x_i^{-1} es también cuadrado.

luego

$$\prod_{i=1}^{s} x_i \equiv 1 \, mod\, p$$

Entonces tendremos

$$\begin{aligned} x_1 \cdot x_s a x_1 \cdots a x_s &= a^s (x_1 \cdots x_s)^2 \\ &\equiv a^s \ mod\ p. \end{aligned}$$

Comparando ambos resultados se tiene

$$a^{\frac{p-1}{2}} \equiv -1 \, mod \, p \qquad \spadesuit$$

Veamos a continuación algunas aplicaciones del teorema 4.1.2

Ejemplo 3:

Probar que 5 es un resto cuadrático módulo 13.

Solución:

Usando (4.1.2) con $a = 5$ y $t = 3$ tenemos

$$\begin{aligned} \left(\frac{5}{13}\right) &\equiv 5^{(13-1)/2} \, mod \, 13 \\ &\equiv 5^6 \, mod \, 13 \\ &\equiv 15625 \, mod \, 13 \\ &\equiv 12 \, mod \, 13 \\ &\equiv -1 \, mod \, 13 \end{aligned}$$

Luego

$$\left(\frac{5}{13}\right) = -1$$

Teorema 4.1.3 *Sea p un número primo y a y b dos enteros primos relativos con* $(a, p) = 1$ *y (b,p)=1. Entonces*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Demostración:

Por intermedio del teorema 4.1.2 se obtiene

$$\begin{aligned}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) &\equiv a^{(p-1)/2}b^{(p-1)/2}\, mod\, p \\ &\equiv (ab)^{(p-1)/2}\, mod\, p \\ &\equiv \left(\frac{ab}{p}\right) mod\, p\end{aligned}$$

Nótese que los posibles valores de los términos en la congruencia

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) mod\, p$$

son todos ± 1, luego la congruencia anterior se convierte en igualdad con lo cual se obtiene el resultado.

♠

Teorema 4.1.4 *Si* $(a, b) = 1$ *y* $(c, p) = 1$ *se tiene*

$$\left(\frac{c^2 a}{p}\right) = \left(\frac{a}{p}\right)$$

Demostración:

Usando el teorema 4.1.3 , se obtiene

$$\left(\frac{c^2 a}{p}\right) = \left(\frac{c^2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)$$

Ejemplo 6:

Calcular $\left(\frac{70}{11}\right)$.

Solución:

Aplicando las propiedades vistas en los ejemplos anteriores se tiene

$$\left(\frac{70}{11}\right) = \left(\frac{7}{11}\right)\left(\frac{5}{1}\right)\left(\frac{2}{11}\right)$$

Para calcular estos tres valores del lado derecho de la igualdad, construimos una tabla de cuadrados módulo 11:

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	10

Usando los valores de la tabla, calculamos los símbolos de Legendre por inspección directa.

$$\left(\frac{7}{11}\right) = -1 \ , \ \left(\frac{5}{11}\right) = 1 \ , \ \left(\frac{2}{11}\right) = -1$$

luego

$$\left(\frac{70}{11}\right) = 1.$$

En la próxima sección, veremos un método más eficiente para calcular símbolos de Legendre sin necesidad de usar tablas.

Ejercicios

1) Sea p un número primo.

a) Probar que en $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, la mitad de los elementos son cuadrados y la otra mitad son no cuadrados.

b) Si a es no cuadrado y $x_1, \cdots, x_s$ son los cuadrados de $\mathbb{Z}_p^*$ entonces $ax_1, \cdots, ax_s$, son todos los no cuadrados de $\mathbb{Z}_p^*$.

2) Demostrar

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)=0$$

3) Calcular

a) $\left(\frac{10}{3}\right)$ b) $\left(\frac{100}{5}\right)$ c) $\left(\frac{200}{3}\right)$

d) $\left(\frac{34}{7}\right)$ e) $\left(\frac{-10}{7}\right)$ f) $\left(\frac{80}{13}\right)$

4) Decidir cuáles de las siguientes ecuaciones posee solución

a) $x^2 \equiv 5 \ mod\ 13$

b) $x^2 \equiv -3 \ mod\ 7$

c) $x^2 \equiv -4 \ mod\ 19$

d) $x^2 \equiv 2 \ mod\ 7$

4.2 Ley de Reciprocidad Cuadrática

Comenzaremos por estudiar algunos resultados preliminares, que necesitamos para demostrar la Ley de Reciprocidad cuadrática.

Definición 4.2.1 *Sea x un número real cualquiera. La parte entera de x que se denota por $[x]$, se define como aquel entero n, tal que*

$$n \leq x < n+1$$

Ejemplos

$$[3,5]=3 \ ; \ [12]=12 \ ; \ [-3,1]=-4$$

Ejercicio:

Para todo real x se cumple.

$$x=[x]+\alpha \quad \text{con} \quad 0 \leq \alpha < 1.$$

Teorema 4.2.1 *Si m es un entero y x es real, se tiene*

$$[x+m] = [x] + [m]$$

Demostración:

De acuerdo al ejercicio anterior se debe cumplir

$$x = [x] + \alpha \quad , \quad 0 \leq \alpha < 1$$

luego

$$x + m = [x] + m + \alpha = t + \alpha,$$

donde $t = [x] + m$

Nótese que t es un entero y además satisface

$$t \leq x + m < t + 1$$

por lo tanto se debe tener

$$[x+m] = t = [x] + m$$

♠

Teorema 4.2.2 *Sean a y b enteros positivos. Entonces existe r tal que*

$$a = b\left[\frac{a}{b}\right] + r \quad , \quad 0 \leq r < b$$

Demostración:

De acuerdo al algoritmo de división, existen r y q tales que

$$a = bq + r \quad , \quad 0 \leq r < b \qquad (*)$$

Luego $a/b = q + (r/b)$. Nótese que q es un entero y además $0 \leq (r/b) < 1$.

Luego debemos tener

$$\left[\frac{a}{b}\right] = q$$

y al sustituir la útima relación en $(*)$ se obtiene el resultado.

♠

En lo sucesivo p y q serán dos números primos distintos. También pondremos

$$s = (p-1)/2 \quad \text{y} \quad t = (q-1)/2$$

Teorema 4.2.3 *(Lema de Gauss) Sea a entero positivo y p un número primo tal que $(a,p) = 1$ y sea K el número de residuos módulo p, mayores que $p/2$ en el conjunto $\{a, 2a, \cdots, sa\}$. Entonces*

$$\left(\frac{a}{p}\right) = (-1)^K$$

Demostración:

El conjunto $\mathcal{A} = \{a, 2a, \cdots, sa\}$ se divide en dos partes

$$\mathcal{A}_r = \{x \in \mathcal{A} \mid x \equiv r_i \, mod \, p \quad , \quad 0 < r_i < p/2\}$$

y

$$\mathcal{A}_s = \{x \in \mathcal{A} \mid s_i \equiv r_j \, mod \, p \quad , \quad s_i > p/2\}$$

Sea $H = s - K$. Afirmamos que

$$r_1, r_2, \cdots, r_H, p - s_1, p - s_2, \cdots, p - s_K \qquad (*)$$

son todos elementos del conjunto $\{1, 2, 3, \cdots, s\}$

En primer lugar, notemos que los elementos en $(*)$ son todos mayores que cero y menores que $p/2$. Además, hay s de ellos. Luego si

podemos demostrar que esos s elementos son todos distintos, la afirmación quedará probada. Tenemos tres casos a considerar:

Caso I) Si $r_i = r_j$, para algunos i, j, entonces, existen $1 \leq R_i, R_j \leq s$, tales que

$$aR_i \equiv aR_j \ mod \ p.$$

Luego p divide a $a(R_i - R_j)$, lo cual implica que p divide a $R_i - R_j$, pues $(a, b) = 1$. Notemos ahora que

$$-p < R_i - R_j < p \quad y \quad R_i \equiv R_j \ mod \ p.$$

Estas dos condiciones se sastifacen, si y sólo si $R_i = R_j$, de donde se obtiene $i = j$.

Caso II) Si $p - s_i = p - s_j$, se obtiene $s_i = s_j$, y usando el mismo argumento del caso I, se deduce $i = j$.

Caso III) Si $r_i = p - s_j$ se sigue entonces

$$r_i \equiv -s_j \ mod \ p,$$

o sea,

$$aR_i \equiv -aS_j \ mod \ p,$$

con $1 \leq R_i, \ S_j \leq s$

Cancelando a en la última ecuación produce:

$$R_i + S_j \equiv 0 \ mod \ p$$

lo cual es imposible, pues R_i y S_j son dos elementos distintos del conjunto $\{1, 2, \cdots, s\}$ con $s = (p-1)/2$.

Por útimo concluimos $r_i \neq p - s_j$.

Con esto queda probada la afirmación.

Seguidamente, consideremos el producto de todos los elementos en $(*)$. Dicho producto resulta ser igual a el producto $1 \cdot 2 \cdots s = s!$, por la afirmación anterior. Se tiene entonces

$$\begin{aligned} s! &= (r_1 \cdots r_H)(p - s_1) \cdots (p - s_K) \\ &\equiv (-1)^K r_1 \cdots r_H s_1 \cdots s_K \, mod \, p. \end{aligned}$$

De donde

$$(-1)^K s! \equiv r_1 \cdots r_H s_1 \cdots s_K \ mod \ p \tag{4.5}$$

Por otro lado

$$\begin{aligned} s! a^s &\equiv (aR_1) \cdots (aR_H)(aS_1) \cdots (aS_K) \, mod \, p \\ s! a^s &\equiv r_1 \cdots r_H s_1 \cdots s_K \, mod \, p \end{aligned} \tag{4.6}$$

Igualando las ecuaciones (4.5) y (4.6) tenemos

$$s! a^s \equiv (-1)^K \ mod \ p$$

Como $1, 2, \cdots, s$ son primos relativos con p, tenemos $(s!, p) = 1$ y por lo tanto podemos cancelar $s!$ en la ecuación anterior, luego

$$a^s \equiv (-1)^K \ mod \ p.$$

Por lo tanto

$$\left(\frac{a}{p}\right) \equiv (-1)^K \ mod \ p$$

♠

Ejemplo:

Usar el lema de Gauss para calcular $\left(\frac{5}{31}\right)$.

Tenemos que $s = \frac{31 - 1}{2} = 15$ y $\frac{p}{2} = 15.5$.

Sea $L = \{5, 2 \cdot 5, 3 \cdot 5, \ldots, 15 \cdot 5\}$, los residuos módulo 31 de los elementos de L son

$$\overline{L} = \{5, 10, 15, 20, 25, 30, 4, 9, 14, 19, 24, 29, 3, 8, 13\}.$$

Luego el conjunto de los elementos de $\overline{L}$ mayores que 15.5 viene dado por

$$A = \{19, 20, 24, 25, 29, 30\}$$

Tenemos entonces, que el número de elementos de A es igual a 6 y por lo tanto $K = 6$.Luego

$$\left(\frac{5}{31}\right) = (-1)^6 = 1$$

A fin de simplificar las demostraciones introduciremos las siguientes notaciones

$$A = r_1 + r_2 + \cdots r_H \tag{4.7}$$

$$B = s_1 + s_2 + \cdots s_K,$$

con $H + K = s$ y $s = \dfrac{(p-1)}{2}$

$$M = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{sa}{p}\right] \tag{4.8}$$

Lema 4.2.1 *Con las notaciones anteriores se tiene*

$$\frac{(a-1)(p^2-1)}{8} = (M - K)p + 2B.$$

Demostración:

Usando las mismas notaciones del teorema 4.2.3 tenemos:

$$R_i a = p\left[\frac{R_i a}{p}\right] + r_i$$

$$S_j a = p\left[\frac{S_j a}{p}\right] + s_j.$$

Luego

$$\begin{aligned}\sum_{i=1}^{s} ia &= \sum_{i=1}^{H} R_i a + \sum_{j=1}^{K} S_j a \\ &= p\sum_{i=1}^{H}\left[\frac{R_i a}{p}\right] + \sum_{i=1}^{H} r_i + p\sum_{j=1}^{K}\left[\frac{S_j a}{p}\right] + \sum_{j=1}^{K} sj\end{aligned}$$

Después de agrupar los términos en p, y utilizar las fórmulas en (4.1), nos queda

$$\sum_{i=1}^{s} ia = pM + A + B.$$

Por otro lado

$$\sum_{i=1}^{s} i = \frac{s(s+1)}{2} = \frac{p^2-1}{8}, \tag{4.9}$$

luego se tendrá

$$\frac{a(p^2-1)}{8} = pM + A + B. \tag{4.10}$$

De acuerdo a la demostración del teorema 4.2.3, se deduce

$$\begin{aligned}\sum_{i=1}^{s} i &= \sum_{i=1}^{H} r_i + \sum_{j=1}^{K} p - s_j \\ &= A + Kp - B.\end{aligned}$$

Luego, podemos usar la ecuación anterior y (4.2), para obtener

$$\frac{p^2-1}{8} = A + Kp - B. \tag{4.11}$$

Restando (4.4) de (4.3) queda

$$\frac{(a-1)(p^2-1)}{8} = (M-K)p + 2B,$$

con lo cual terminamos la demostración ♠

En el desarrollo de la prueba del lema anterior se obtuvo el siguiente resultado (ver ecuación 4.11).

Lema 4.2.2 *Si $p \neq 2$ es primo, entonces*

$$\frac{p^2-1}{8}$$

es un entero.

El siguiente lema permite calcular el símbolo de Legendre $\left(\frac{a}{p}\right)$, para el caso especial $a = 2$.

Lema 4.2.3

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

Demostración:

Haciendo $a = 2$ en (4.9), se tiene

$$\frac{p^2-1}{8} = (M-K)p + 2B.$$

Podemos calcular el valor de M, directamente de la definición

$$M = \left[\frac{2}{p}\right] + \left[\frac{4}{p}\right] + \cdots + \left[\frac{s2}{p}\right].$$

Obsérvese ahora, que cada uno de los términos que aparece dentro de los corchetes son mayores de cero y menores que uno, luego podemos concluir: $M = 0$.

Por lo tanto

$$\begin{aligned} \frac{p^2-1}{8} &= -Kp + 2B \\ &\equiv -Kp \, mod \, 2 \\ &\equiv K \, mod \, 2. \end{aligned}$$

Finalmente, usando el lema de Gauss se obtiene

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

Con esto terminamos la demostración. ♠

Ejemplo:

Calcular $\left(\frac{2}{13}\right)$.

Solución:

$$\left(\frac{2}{13}\right) = (-1)^{169-1)/2} = (-1)^2 1 = -1.$$

Seguidamente, damos una fórmula para obtener el símbolo de Legendre $\left(\frac{q}{p}\right)$, donde q es primo ($q \neq p \quad , \quad q \neq 2$).

Teorema 4.2.4 *Sean p y q dos números primos diferentes. Entonces*

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

donde

$$M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots \left[\frac{sq}{p}\right].$$

Demostración:

Tomando $a = q$ en el lema (4.2.3), se tiene

$$\frac{(q-1)(p^2-1)}{8} = (M-K)p + 2B.$$

Por ser q impar y $(p^2-1)/8$ entero, se deduce de lo anterior

$$(M-K)p \equiv 0 \ mod\ 2.$$

Usando el hecho $(p, 2) = 1$, obtenemos

$$M \equiv k \ mod\ 2.$$

Combinando esta útima ecuación con el lema de Gauss se deduce el resultado

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

♠

Observación: Si en la ecuación anterior, se intercambian p y q obtenemos

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

donde

$$N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{tp}{q}\right]$$

$t = (q-1)/2$.

El resultado siguiente es clave para la demostración de la Ley de Reciprocidad Cuadrática.

Lema 4.2.4 *Con las notaciones anteriores se tiene*

$$M + N = s.t.$$

Demostración:

La idea de la demostración es de tipo geométrico, y se debe a Einsenstein, un discípulo de Gauss.

Consideramos un sistema de coordenadas cartesianas en el plano, y sean los puntos $O = (0, 0)$, $A = (p/2, 0)$, $B = (0, q/2)$ y $C = (p/2, q/2)$.

Sea L el conjunto de puntos de coordenadas enteras, dentro del rectángulo $\square OACB$ (ver el diagrama).

Afirmamos que no hay puntos de L sobre la diagonal. La ecuación de la misma esta dada por:

$$py = qx$$

Si (x_1, y_1) es un punto L sobre la diagonal, se cumple $py_1 = qx_1$, lo cual implica que p divide a x_1. Esto es una contradicción pues $1 \leq x_1 < p/2$. Por lo tanto la afirmación es válida.

A continuación contaremos el número de puntos de L, el cual será denotado por ℓ, de dos formas distintas:

Forma I): Sea ℓ = puntos dentro del triángulo $\triangle OAC$+ puntos localizados dentro del triángulo $\triangle OBC$.

Sea λ_r, $1 \leq r \leq s$, el número de puntos de L dentro del triángulo $\triangle OAC$ y sobre la línea $x = r$, luego es fácil ver que

$$\lambda_r = \left[\frac{rq}{p}\right] \quad , \quad 1 \leq r \leq s.$$

Si sumamos sobre r obtenemos:

$$\text{puntos dentro del triángulo } \triangle OAC = \sum_{r=1}^{s} \lambda_r = M.$$

De la misma forma se demuestra:

$$\text{puntos dentro del triángulo } \triangle OBC = N.$$

Luego

$$\ell = M + N.$$

Forma II): Por otro lado, viendo a L como un rectángulo se tiene:

$$\ell = \text{puntos en la base} \times \text{puntos en la altura} = s \cdot t.$$

Comparando ambos resultados, se deduce

$$M + N = s \cdot t.$$

♠

Teorema 4.2.5 *(Ley de Reciprocidad Cuadrática) Sean p y q dos primos impares distintos, entonces*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}} \tag{4.12}$$

Demostración:

En el teorema 4.2.5 hemos probado

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

De esto se sigue

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N} = (-1)^{st} \quad 4.11,$$

lo cual nos conduce al resultado deseado, al hacer la sustitución

$$s = \frac{p-1}{2} \quad \text{y} \quad t = \frac{q-1}{2}$$

♠

Observación : La Ley de Reciprocidad Cuadrática puede ser escrita de otra manera. Podemos multiplicar la ecuación (4.12) por $\left(\frac{q}{p}\right)$ para obtener

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

Ejemplo:

Calcular $\left(\frac{13}{37}\right)$, usando la Ley de Reciprocidad Cuadrática.

Solución:

Denotemos por LRC="Ley de Reciprocidad Cuadrática".

$$\begin{aligned}\left(\frac{13}{37}\right) &= (-1)^{\frac{13-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{13}\right) \quad \text{(por LRC)} \\ &= \left(\frac{37}{13}\right) \\ &= \left(\frac{11}{13}\right),\end{aligned}$$

pero

$$\begin{aligned}\left(\frac{11}{13}\right) &= (-1)^{\frac{11-1}{2}\cdot\frac{13-1}{2}}\left(\frac{13}{11}\right) \quad \text{(por LRC)}\\ &= \left(\frac{13}{11}\right)\\ &= \left(\frac{2}{11}\right)\\ &= (-1)^{(11^2-1)/8} \quad \text{por} \quad (4.11)\\ &= (-1)^{15}\\ &= -1.\end{aligned}$$

Ejemplo:

Decidir si la congruencia

$$x^2 \equiv 5 \; mod \; 227,$$

es soluble.

Solución:

La congruencia será soluble si y sólo si 5 es un resto cuadrático módulo 227; si sólo si

$$\left(\frac{5}{227}\right) = 1.$$

Evaluando este símbolo, tenemos

$$\begin{aligned}\left(\frac{5}{227}\right) &= (-1)^{\frac{5-1}{2}\cdot\frac{227-1}{2}}\left(\frac{227}{5}\right)\\ &= \left(\frac{227}{5}\right)\\ &= \left(\frac{2}{5}\right)\\ &= (-1)^{(5^2-1)/8}\\ &= -1.\end{aligned}$$

Concluimos entonces que la ecuación no es soluble.

4.3 Símbolo de Jacobi

El símbolo de Legendre $\left(\frac{a}{p}\right)$, se define únicamente para p, un número primo. En esta sección, daremos una generalización de este símbolo, en donde el "denominador" p, puede ser un número compuesto.

Definición 4.3.1 *Sean a y b dos enteros primos relativos, y además b tiene descomposición como producto de primos $b = p_1 \cdot p_2 \cdots p_n$, donde los p_i no son necesariamente distintos. Entonces el* **símbolo de Jacobi** $\left(\frac{a}{b}\right)$, *se define por*

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{n} \left(\frac{a}{p_i}\right),$$

donde $\left(\frac{a}{p_i}\right)$ es el símbolo de Legendre.

Ejemplo:

$$\left(\frac{7}{15}\right) = \left(\frac{7}{3}\right)\left(\frac{7}{5}\right)$$

Observación: Si p es un número primo, entonces el símbolo de Jacobi y el símbolo de Legendre, cuando p va en la parte inferior, son indistinguibles.

Observación: Si b es compuesto, entonces la notación $\left(\frac{a}{b}\right) = 1$, no implica necesariamente que a sea un resto cuadrático módulo b.

Por ejemplo $\left(\frac{5}{9}\right) = 1$, pero no existe x tal que $x^2 \equiv 5 \ mod\ 9$.

El símbolo de Jacobi goza de muchas propiedades similares a las del símbolo de Legendre.

Teorema 4.3.1 *Sean a, b, c y d enteros tales que $(a, c) = 1$. Entonces*

1) $\left(\frac{a}{b}\right)\left(\frac{a}{d}\right) = \left(\frac{a}{bd}\right)$

2) $\left(\frac{a}{b}\right)\left(\frac{c}{b}\right)=\left(\frac{ac}{b}\right)$

3) $\left(\frac{a^2}{b}\right)=1$

4) $\left(\frac{a}{b^2}\right)=1$

5) $\left(\frac{ac^2}{b}\right)=\left(\frac{a}{b}\right)$

Demostración:

Ejercicio.

♠

Teorema 4.3.2 *Si b es impar positivo, se cumple:*

$$\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$$

Demostración:

En efecto, sea $b = p_1 \cdot p_2 \cdots p_n$. Usando la definición del símbolo de Jacobi se tiene

$$\begin{aligned}\left(\frac{2}{b}\right) &= \prod_{i=1}^{n}\left(\frac{2}{p_i}\right)\\ &= \prod_{i=1}^{n}(-1)^{(p_i^2-1)/8}\\ &= (-1)^{\alpha},\end{aligned}$$

donde $\alpha = \sum_{i=1}^{n}(p_i^2-1)/8$.

Para nuestros propósitos, será suficiente conocer el valor de α módulo 2. Observar que si p_1 y p_2 son primos, entonces

$$\begin{aligned}\frac{p_1^2p_2^2-1}{8}-\left[\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}\right] &= \frac{(p_1^2-1)(p_2^2-1)}{8}\\ &\equiv 0\, mod\, 2.\end{aligned}$$

Luego

$$\frac{p_1^2p_2^2-1}{8}\equiv\left(\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}\right)\, mod\, 2.$$

Aplicando esta última identidad a los restantes primos p_i, nos da

$$\frac{\prod_{i=1}^n p_i^2-1}{8}\equiv\sum_{i=1}^n\frac{(p_i^2-1)}{8}\equiv\ mod\ 2.$$

Por lo tanto concluimos

$$\alpha\equiv\ \frac{\prod_{i=1}^n p_i^2-1}{8}\ mod\ 2,$$

esto es

$$\alpha\equiv\ \frac{b^2-1}{8}\ mod\ 2,$$

de donde se obtiene

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

♠

Seguidamente, pasamos a ver la Ley de Reciprocidad Cuadrática, para el símbolo de Jacobi.

Teorema 4.3.3 *Si a y b son enteros positivos impares primos entre sí, se tiene*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

Demostración:

Supongamos que $a = p_1 \cdot p_2 \cdot p_n$, y $b = q_1 \cdot q_2 \cdots q_m$, entonces

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i=1}^{m}\left(\frac{a}{q_i}\right)\prod_{j=1}^{n}\left(\frac{b}{p_j}\right) \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}(-1)^{\frac{p_j-1}{2}\cdot\frac{q_i-1}{2}} \\ &= (-1)^{\beta},\end{aligned}$$

donde

$$\begin{aligned}\beta &= \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{p_j-1}{2}\cdot\frac{q_i-1}{2} \\ &= \left[\sum_{j=1}^{n}\frac{p_j-1}{2}\right]\left[\sum_{i=1}^{m}\frac{q_i-1}{2}\right]\end{aligned}$$

Interesa entonces calcular el valor de β módulo 2, para lo cual

$$\frac{p_1p_2-1}{2} - \left\{\left[\frac{p_1-1}{2}\right] + \left[\frac{p_2-1}{2}\right]\right\} = \frac{(p_1-1)(p_2-1)}{2} \equiv 0\, mod\, 2,$$

luego

$$\frac{p_1p_2-1}{2} \equiv \frac{(p_1-1)}{2} + \frac{(p_2-1)}{2}\ mod\ 2.$$

Haciendo uso de esta última congruencia, tantas veces como se requiera, produce

$$\frac{p_1p_2\cdots p_n-1}{2} \equiv \sum_{i=1}^{n}\frac{p_i-1}{2}\ mod\ 2.$$

o sea

$$\frac{a-1}{2} \equiv \sum_{i=1}^{n}\frac{(p_i-1)}{2}\ mod\ 2.$$

De igual forma, se obtiene un resultado análogo para b.

$$\frac{b-1}{2} \equiv \sum_{i=1}^{n} \frac{(q_j-1)}{2} \ mod\ 2.$$

Por lo tanto

$$\beta \equiv \frac{(a-1)}{2} \cdot \frac{(b-1)}{2} \ mod\ 2,$$

y con esto finaliza la demostración. ♠

Ejercicios

1) Calcular

$$i)\left(\frac{5}{37}\right) \quad ii)\left(\frac{2}{37}\right) \quad iii)\left(\frac{10}{37}\right) \quad iv)\left(\frac{100}{101}\right) \quad v)\left(\frac{50}{13}\right)$$

2) Determinar cuáles de las siguientes congruencias tienen solución:

i) $x^2 \equiv -2 \ mod\ 59$

ii) $x^2 \equiv 2 \ mod\ 59$

iii) $x^2 \equiv -2 \ mod\ 41$

iv) $x^2 \equiv 2 \ mod\ 37$

v) $x^2 \equiv 2 \ mod\ 101$

3) Demostrar que para todo primo p se tiene:

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0.$$

4) Demuestre que si las ecuaciones $x^2 \equiv a \ mod\ p$ y $x^2 \equiv b \ mod\ p$ no son solubles, entonces $x^2 \equiv ab \ mod\ p$ es soluble.

5) Probar que $x^2 \equiv 2 \ mod\ p$ es soluble ($p \neq 2$), si y sólo si $p \equiv 1 \text{ ó } 7 \ mod\ 8$.

6) Si p es primo, $p \neq 2$. Probar $p^4 - 1 \equiv 0 \ mod\ 16$.

7) Sea $\mathcal{A}$ = conjunto de restos cuadráticos $mod\, p$ y $\mathcal{B}$ = al conjunto de restos no cuadráticos $mod\, p$. Probar:

i) aa' está en $\mathcal{A}$, para todo a y a' en $\mathcal{A}$.

ii) bb' está en $\mathcal{A}$, para todo b y b' en $\mathcal{B}$.

iii) ab está en $\mathcal{B}$, para todo a en $\mathcal{A}$ y b en $\mathcal{B}$.

8) Usando el problema anterior, demostrar $\|\mathcal{A}\| = \|\mathcal{B}\| = (p-1)/2$.

9) Probar

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

10) Usando la Ley de Reciprocidad Cuadrática, decidir cuáles de las siguientes ecuaciones tienen solución:

i)$x^2 \equiv 15 \ mod\ 103$

ii)$x^2 \equiv 20 \ mod\ 167$

iii)$x^2 \equiv -6 \ mod\ 157$

iv)$x^2 \equiv 8 \ mod\ 479$.

11) Probar que si $p \equiv 1 \ mod\ 4$, entonces

$$x^2 \equiv p \ mod\ q \text{ es soluble si y sólo si } x^2 \equiv q \ mod\ p \text{ lo es}$$

12) Usando el ejercicio 11) demuéstrese que si $p \equiv 1 \ mod\ 10$, entonces

$$\left(\frac{10}{p}\right) = 1.$$

13) Probar el recíproco del teorema de Wilson:
"Si $(p-1)! \equiv -1 \ mod\ p$, entonces p es primo".

14) Demuéstrese el teorema 4.3.1

15) Para cuáles primos p la congruencia:

$$x^2 \equiv -1 \ mod\ p$$

es soluble.

16) Mostrar que si p y q son dos primos diferentes de dos, entonces

$$\frac{(p^2-1)(q^2-1)}{8} \ \equiv \ 0 \ mod\ 2.$$

Capítulo

5

Fracciones Continuas

5.1 Introducción

Las fracciones continuas son uno de los temas más interesantes dentro de la teoría de números, así como también uno de los más antiguos. Su origen se remonta a la antigua Grecia, específicamente **Euclides** estudió por primera vez este tipo particular de fracciones en el Libro 8 de *los Elementos*. Euclides vivió en el siglo 3 a.c. y enseñó matemáticas en Alejandría.

En la Edad Moderna la teoría fue retomada por el matemático italiano **Bombelli**, en su libro *L'Algebra parte maggiore dell' aritmetica*. Bologna 1572, en donde se utilizan fracciones continuas para calcular raíces cuadradas.

Por ejemplo

$$\sqrt{13} = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cdots}}$$

Posteriormente **Leonhard Euler** en su memoria *De fractionibus continuis. 1737* , dio los primeros pasos en la teoría, tal como se conoce en la actualidad.

Finalmente, fue el célebre matemático francés **Joseph Louis Lagrange** quien en 1768 formalizó esta teoría en su memoria *Solution d'un problème d'arithmétique*. Lagrange resolvió completamente la famosa ecuación de Fermat

$$x^2 - dy^2 = 1$$

para lo cual usó de manera esencial las fracciones continuas.

5.2 Fracciones Continuas

Definición 5.2.1 *Sean $a_0, a_1, \ldots, a_n, \ldots$ números reales no nulos. Una expresión del tipo*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

se llama **Fracción Continua**

Notación Para denotar la expresión de arriba, usaremos el símbolo:

$$[a_0, a_1, \ldots, a_n, \ldots].$$

Definición 5.2.2 *Sean $a_1, \ldots, a_n$ números reales. Entonces la expresión*

$$[a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{n-1} + \cfrac{1}{a_n}}}$$

se llama **Fracción Continua Finita** .

Observación : Usualmente los a_i, en la descomposición de una fracción continua son números enteros positivos. En tal caso diremos que la fracción continua es **simple**.

Podemos representar una fracción continua infinita, como el límite de una fracción continua finita. Esto es

$$[a_0, \ldots, a_n, \ldots] = \lim_{n\to\infty} [a_0, \ldots, a_n]$$

Estudiaremos para cada n, el número racional generado por la expansión de $[a_0, \ldots, a_n]$. Así pues tenemos

$$[a_0] = a_0 = \frac{a_0}{1}$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1}$$

$$[a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1}$$

etc...

En general sea

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Entonces p_n y q_n se llaman las **convergentes n-ésimas** de la fracción continua dada. Es claro que tanto p_n como q_n son polinomios que dependen de $a_0, \ldots, a_n$. Tenemos entonces las siguientes expresiones para estos polinomios

$$p_0 = a_0, \quad p_1 = a_1 a_0 + 1, \quad , p_2 = a_2 a_1 a_0 + a_2 + a_0, \quad \ldots$$

$$q_0 = 1, \quad q_1 = a_1, \quad q_2 = a_2 a_1 + 1, \quad \ldots$$

Teorema 5.2.1 *Para todo $n \geq 2$ se tiene*

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_n = a_n q_{n-1} + q_{n-2}$$

Demostración:

Usaremos inducción sobre n. Para $n = 2$, el resultado es cierto. Supongamos que el resultado es válido para n. Entonces

$$[a_0, \ldots, a_n, a_{n+1}] = [a_0, \ldots, a_{n-1}, a_n + 1/a_{n+1}]$$

Es claro que la (n+1)-ésima convergente de la fracción de la izquierda es igual a la n-ésima convergente de la fracción de la derecha. Luego

$$\begin{aligned}\frac{p_{n+1}}{q_{n+1}} &= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \\ &= \frac{a_{n+1}a_n p_{n-1} + p_{n-1} + a_{n+1}p_{n-2}}{a_{n+1}a_n q_n + q_{n-1} + a_{n+1}q_{n-2}}\end{aligned}$$

Usando ahora la hipótesis de inducción se tiene

$$\begin{aligned}\frac{p_{n+1}}{q_{n+1}} &= \frac{a_{n+1}(p_n - p_{n-2}) + p_{n-1} + a_{n+1}p_{n-2}}{a_{n+1}(q_n - q_{n-2}) + q_{n-1} + a_{n+1}q_{n-2}} \\ &= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}\end{aligned}$$

Con esto termina la demostración. ♠

Podemos construir un algoritmo para generar las convergentes de una fracción continua, mediante una tabla

n	a_{n+1}	p_n	q_n
0	a_1	a_0	1
1	a_2	p_1	q_1
2	a_3	p_2	q_2

Iniciamos la tabla colocando los valores de $a_0, a_1, a_2, p_0, p_1, q_0$ y q_1. Luego a partir de $n = 2$, para hallar el valor de p_n procedemos de la forma siguiente: Se toma el elemento en la casilla superior, éste se multiplica por el de la casilla de la izquierda y luego se le suma el de la casilla de arriba. Los q_n se hallan de la misma forma.

Ejemplo: Hallar la décima convergente de la fracción continua

$$[2, 1, 2, 1, 2, \ldots]$$

Tenemos entonces la tabla

n	a_{n+1}	p_n	q_n
0	1	2	1
1	2	3	1
2	1	8	3
3	2	11	4
4	1	30	11
5	2	41	15
6	1	112	41
7	2	153	56
8	1	418	153
9	2	571	209
10	1	1560	571

Calcularemos los valores de las fracciones $x_n = p_n/q_n$ cuando n toma los valores: $0, \cdots, 10$. Esto nos da el siguiente resultado:

x_0	2
x_1	3
x_2	2.66667
x_3	2.75
x_4	2.7272
x_5	2.7333
x_6	2.73171
x_7	2.73214
x_8	2.73202
x_9	2.73206
x_{10}	2.73205

Mirando la última tabla se puede intuir que las fracciones p_n/q_n convergen a un límite. La demostración de este hecho en general no es fácil y requiere de una serie de resultados previos que daremos a continuación.

Proposición 5.2.1 *Para todo $n \geq 1$ se tiene*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \tag{5.1}$$

Demostración:

Usando el teorema 5.2.1 se tiene

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \end{aligned}$$

Si aceptamos la hipótesis de inducción para $n-1$, la cual establece

$$(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (-1)^{n-2}$$

se tendrá entonces

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

♠

Si en la ecuación anterior dividimos ambos miembros entre $q_n q_{n-1}$, obtenemos

Proposición 5.2.2 *Para todo $n \geq 1$ se tiene*

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \tag{5.2}$$

Proposición 5.2.3 *Para todo $n \geq 1$ se tiene*

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n \tag{5.3}$$

Demostración:

Usando el Teorema 5.2.1 se tiene

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= a_n (-1)^{n-2} \quad por \quad (5.1) \\ &= (-1)^n a_n \end{aligned}$$

♠

Observación: En lo sucesivo sólo consideramos fracciones continuas en donde los elementos $a_0, \ldots a_n, \ldots$ son números enteros positivos. Estas se llaman **Fracciones continuas simples**.

Teorema 5.2.2 *Toda fracción continua simple es convergente a un número real.*

Demostración:

Sea $x = [a_0, a_1, \ldots]$ y para $n \geq 1$ sea

$$x_n = [a_0, \ldots a_n] = \frac{p_n}{q_n}$$

Probaremos que la sucesión x_n converge a un límite L, lo cual será hecho en varias etapas.

1. *La subsucesión x_{2n} de términos pares es monótona estrictamente creciente. La subsucesión x_{2n+1} de términos impares es monótona estrictamente decreciente.*

   En efecto, de (5.3) obtenemos

   $$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = (-1)^n a_n$$

   luego si n es par

$$\frac{p_n}{q_n} > \frac{p_{n-2}}{q_{n-2}}$$

y si n es impar

$$\frac{p_n}{q_n} < \frac{p_{n-2}}{q_{n-2}}.$$

Por lo tanto la subsucesión $\{x_{2n}\}$ es creciente y la subsucesión $\{x_{2n-1}\}$ es decreciente.

2. *Las subsucesiones de términos pares e impares, respectivamente, son convergentes*

   De la relación (5.2) deducimos

$$x_{2n} - x_{2n-1} < 0$$

   luego

$$x_{2n} < x_{2n-1}$$

   Como $\{x_{2n}\}$ es creciente y $\{x_{2n-1}\}$ es decreciente, se obtiene la interesante relación

$$x_2 < x_{2n} < x_{2n-1} < x_1 \quad \text{para todo } n \geq 1.$$

   Como consecuencia de todo esto se obtiene que $\{x_{2n}\}$ es monótona creciente acotada, luego es convergente.

   Sea

$$\lim_{n\to\infty} x_{2n} = L_1$$

   De igual forma, $\{x_{2n-1}\}$ es monótona decreciente acotada y por lo tanto convergente.

Sea

$$\lim_{n\to\infty} x_{2n-1} = L_2$$

3. *La sucesión* $\{x_n\}$ *es convergente .*

   De la relación (5.2) se obtiene

$$\mid x_n - x_{n-1} \mid = \frac{1}{q_n q_{n-1}} \leq \frac{1}{n^2}.$$

   Por lo tanto la sucesión $\{x_n\}$ es una sucesión de Cauchy. Esto es, a medida que n crece, la distancia entre los términos se hace más pequeña. Luego la sucesión es convergente a un límite L, y además toda subsucesión convergente de ella, converge al mismo límite. Por lo tanto $L_1 = L_2 = L$, y

$$\lim_{n\to\infty} x_n = L$$

♠

Teorema 5.2.3 *Toda fracción continua simple finita* $[a_0, \ldots a_n]$ *representa un número racional.*

Demostración:

Basta observar que

$$[a_0, \ldots a_n]$$

se puede escribir como

$$a_0 + 1/[a_1, \ldots a_n].$$

Luego, aplíquese inducción sobre n.

♠

Teorema 5.2.4 *Toda fracción racional $\alpha = p/q$ se expresa como una fracción continua simple finita.*

Nota: No hay unicidad en esta representación, pues

$$[a_0, \dots a_n] = [a_0, \dots, a_{n-1}, a_n - 1, 1]$$

Sin embargo éstas son las dos únicas representaciones posibles de α.

Demostración:

Usaremos la notación: $[x]$ para indicar la parte entera de un número real x. Comenzamos por hacer

$$r_0 = \alpha \quad r_1 = \frac{1}{r_0 - [r_0]}, \dots r_n = \frac{1}{r_{n-1} - [r_{n-1}]} \tag{5.4}$$

De aquí se obtiene

$$r_n = [r_n] + \frac{1}{r_{n+1}} \quad \text{para todo } \ n \geq 0$$

Nótese que para todo i, se tiene que $r_i > 1$, luego $1/r_i < 1$ y por lo tanto, los coeficientes a_i de la expansión de α como una fracción continua vienen dados por

$$a_0 = [\alpha], a_1 = [r_1], \dots, a_n = [r_n] \tag{5.5}$$

Por otro lado, usando el algoritmo de división para p y q, se obtiene

$$\begin{aligned}
p &= a_0 q + r_1, \quad 0 \leq r_1 < q \\
q &= a_1 r_1 + r_2, \quad r_2 < r_1 < q \\
r_1 &= a_2 r_2 + r_3, \quad r_3 < r_2 \\
&= \quad \vdots \\
r_i &= a_{i+1} r_{i+1} + r_{i+2}, \quad r_{i+2} < r_{i+1}
\end{aligned}$$

Como $\{r_i\}$ es una sucesión decreciente de enteros positivos, se debe tener eventualmente, $r_{n+1} = 0$ para algún n. Luego el proceso de formación de los a_i se detiene en a_n.

Por lo tanto

$$\alpha = \frac{p}{q} = [a_0, \ldots, a_n]$$

♠

Observación: Si α es un número irracional , entonces la fracción continua asociada a él, se obtiene usando el algoritmo dado en (5.5)

Proposición 5.2.4 *Sea* $\alpha = [a_0, a_1, \ldots, a_n, \ldots]$ *y sean*

$$r_0 = \alpha, \quad r_1 = \frac{1}{r_0 - [r_0]}, \ldots, r_n = \frac{1}{r_{n-1} - [r_{n-1}]}$$

Entonces

$$r_n = [a_n, a_{n+1}, \ldots]$$

Demostración:

Usaremos inducción sobre n. Para $n = 1$, tenemos

$$\alpha = a_0 + \frac{1}{r_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots}}$$

de aquí se concluye que $r_1 = [a_1, a_2, \ldots]$.

Supongamos que el resultado es cierto para n, luego

$$\begin{aligned} r_{n+1} &= \frac{1}{r_n - a_n} \\ &= \frac{1}{[a_n, a_{n+1}, \ldots] - a_n} \\ &= [a_{n+1}, \ldots] \end{aligned}$$

Luego el resultado es cierto para $n+1$. Con esto damos fin a la demostración.

♠

Proposición 5.2.5 *Sea α un número real y r_n la siguiente sucesión de números*

$$r_0 = [\alpha], r_0 = [r_0] + \frac{1}{r_1}, \ldots, r_n = [r_n] + \frac{1}{r_{n+1}}, \quad n \geq 1$$

entonces

$$\alpha = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}}$$

Demostración:

De acuerdo a la demostración del teorema anterior se sigue que $[r_n] = a_n$ para todo n, luego usamos inducción sobre n para probar este resultado.

Si $n = 1$, se tendrá

$$\begin{aligned}
\alpha &= a_0 + \frac{1}{a_1 + \frac{1}{r_2}} \\
&= a_0 + \frac{r_2}{r_2a_1 + 1} \\
&= \frac{(r_2a_1 + 1)a_0 + r_2}{r_2a_1 + 1} \\
&= \frac{r_2a_1a_0 + a_0 + r_2}{r_2a_1 + 1} \\
&= \frac{r_2(a_1a_0 + 1) + a_0}{r_2a_1 + 1} \\
&= \frac{r_2p_1 + p_0}{r_2q_1 + q_0}
\end{aligned}$$

Supongamos que el teorema es cierto para n, y probaremos que se cumple para $n+1$.

Luego

$$\begin{aligned}
\alpha &= \frac{r_n p_{n-1} + p_{n-2}}{r_n q_{n-1} + q_{n-2}} \\
&= \frac{a_n p_{n-1} + p_{n-2} + \dfrac{p_{n-1}}{r_{n+1}}}{a_n q_{n-1} + q_{n-2} + \dfrac{q_{n-1}}{r_{n+1}}} \\
&= \frac{p_n + \dfrac{p_{n-1}}{r_{n+1}}}{q_n + \dfrac{q_{n-1}}{r_{n+1}}} \\
&= \frac{r_{n+1} p_n + p_{n-1}}{r_{n+1} q_n + q_{n-1}}
\end{aligned}$$

♠

Seguidamente daremos una serie de ejemplos en donde calcularemos los elementos de una fracción continua de algunos números.

Ejemplo: Sea $\alpha = \sqrt{2}$, entonces mediante la aplicación del algoritmo dado en la demostración del teorema 5.2.4, calculamos los a_i en la descomposición

$$\alpha = [a_0, a_1, \ldots, a_n, \ldots]$$

En primer lugar, notamos que

$$\alpha = \frac{2}{\alpha} = 1 + \frac{2-\alpha}{\alpha}, \qquad \text{y} \qquad 0 < \frac{2-\alpha}{\alpha} < 1$$

luego $[a_0] = 1$. Para calcular a_1 hacemos

$$\frac{\alpha}{2-\alpha} = \frac{1}{2/\alpha - 1} = \frac{1}{\alpha - 1}$$

Multiplicando numerador y denominador por $(\alpha + 1)$ se tiene

$$\frac{\alpha}{2-\alpha} = \frac{\alpha + 1}{(\alpha - 1)(\alpha + 1)} = \frac{\alpha + 1}{\alpha^2 - 1} = 1 + \alpha$$

de donde $a_1 = [1 + \alpha] = 2$.

Para calcular el siguiente elemento, hacemos

$$\frac{1}{(1+\alpha)-2} = \frac{1}{\alpha - 1} = 1 + \alpha$$

y por lo tanto $a_2 = [1 + \alpha] = 2$.

Continuando de esta manera, vemos que $a_i = 2$, para todo $i \geq 1$.

Luego

$$\sqrt{2} = [1, 2, 2, \ldots]$$

Ejemplo: *Una aplicación en la astronomía: Eclipses lunares.*

Un eclipse lunar se produce cuando la luna penetra en el cono de sombra creado por la tierra, al interponerse ésta entre el sol y la luna.

Los eclipses sólo se producen cuando la luna nueva o llena se encuentra en los llamados nodos ascendentes o descendentes de la órbita que describe alrededor de la Tierra.

Por lo tanto el eclipse depende

1. Del intervalo entre dos fases iguales consecutivas de La Luna, el cual es llamado *Mes Sinódico* y tiene una duración de 29,5306 días.

2. Del intervalo de tiempo entre el paso de la luna por dos nodos consecutivos, el cual se llama *Mes Draconítico* y tiene una duración de 27,2122 días

Luego el intervalo de tiempo entre dos eclipses consecutivos debe ser igual a una cantidad entera de meses sinódicos, que a su vez contenga una cantidad entera de meses draconíticos.

Es decir si

$$x = 29,5306 \quad y \quad z = 27,2123$$

se desea obtener una relación del tipo

$$qx = pz$$

con p y q números enteros positivos.

Esto es, si hacemos

$$\alpha = \frac{x}{z} = 1,08519$$

entonces la pregunta es ¿Cuál es la fracción p/q con menor denominador que está más cercana a 1,08519? Para resolver este problema, usamos fracciones continuas.

En primer lugar, hallamos los coeficientes a_i de la expansión

$$\alpha = [a_0, \ldots, a_n, \ldots]$$

usando el algoritmo del teorema 5.2.4.

En segundo lugar, hallamos las convergentes de esta fracción continua por intemedio del algoritmo del teorema 5.2.1.

Colocando toda esta información en una tabla nos da

n	a_{n+1}	p_n	q_n	p_n/q_n
0	11	1	1	1
1	1	12	11	1.09091
2	2	13	12	1.08333
3	1	38	35	1.08571
4	4	51	47	1.08511
5	2	242	223	1.08520
6	9	535	493	1.08519
7	1	5057	4660	1.08519

Las distintas aproximaciones a α vendrán dadas por los cocientes p_n/q_n . Vemos que el valor 242/223 es aceptable pues difiere de α en 10^{-5} días, lo cual es

$$3600x24x10^{-5}\ sg. = 0.864\ sg.$$

lo cual es depreciable, pues los eclipses tienen una duración promedio de 50 minutos.

Luego se tiene la relación fundamental.

223 meses sinódicos = 242 meses draconíticos

Esta relación, conocida como **Ciclo de Saros**, fue descubierta por los astrónomos de la antigua Mesopotamia.

Finalmente, para calcular el período entre dos eclipses multiplicamos: 223×29.5306 = 6585,3238 días = 18 años y 14 días. Por lo tanto, los eclipses de luna ocurren cada 19 años aproximadamente.

Ejemplo: *El número* π
Podemos hallar algunas aproximaciones de π mediante fracciones continuas. A tal fin tomamos el siguiente valor de este número, el cual es correcto hasta la octava cifra decimal

$$\pi = 3.14159265$$

Luego se tiene

$$\begin{array}{ll} a_0 = [\pi] = 3 & r_1 = 1/(\pi - 3) = 7.0625 \\ a_1 = [r_1] = 7 & r_2 = 1/(r_1 - a_1) = 15.99660 \\ a_2 = [r_2] = 15 & r_3 = 1/(r_2 - a_2) = 1.00341 \\ a_3 = [r_3] = 1 & r_4 = 1/(r_3 - a_3) = 293.09689 \\ a_4 = [r_4] = 293 & r_5 = 1/(r_4 - a_4) = 10.32056 \\ a_5 = [r_5] = 10 & \end{array}$$

Empleamos ahora el algoritmo del Teorema 5.2.1 para hallar las cuatro primeras convergentes de π.

n	a_{n+1}	p_n	q_n	p_n/q_n
0	7	3	1	3
1	15	22	7	3.14285714
2	1	333	106	3.14150943
3	293	355	113	3.14159292
4	10	104348	33215	3.14159265

El valor aproximado de π dado por la quinta convergente es bastante bueno, dado que se aproxima al valor correcto en ocho cifras decimales.

El valor 355/113 fue descubierto por el matemático chino Tsu-Chung-Chi, en el siglo 430 d.c. Durante la Edad Media en Europa, se tomaba 22/7 como el valor correcto de π. Otros autores, en Europa y en la India, usaban la expresión $\sqrt{10}$.

A partir del Renacimiento, con el gran impulso que se le dio a la ciencia, comenzaron a aparecer mejores aproximaciones, e inclusive series de sumas o productos en donde se puede calcular π. Por ejemplo, el matemático francés Vieta, a mediados del siglo XVI, descubrió la fórmula

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}}.\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}.\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}}\cdots$$

A fines del siglo XVII ya se conocía el valor de π con las primeras 50 cifras exactas.

5.3 Facciones continuas periódicas

Definición 5.3.1 *Una fracción continua simple de la forma*

$$\begin{aligned} \alpha &= [a_0, a_1, \ldots, a_n, b_1, \ldots, b_k, b_1, \ldots, b_k, \ldots] \\ &= [a_0, a_1, \ldots, a_n, \ \overline{b_1, \ldots, b_k}\ ] \end{aligned}$$

se dice **Periódica**.

La sucesión de números $b_1, \ldots, b_k$ se llama **el Período de** α . La sucesión de enteros $a_1, \ldots, a_n$ se llama **el Preperíodo de** α. El entero k, se le llama también el período de la fracción continua α.

Definición 5.3.2 *Una fracción continua de la forma*

$$\alpha = [\ \overline{b_1, \ldots, b_k}\ ]$$

se llama **Periódica pura**.

Proposición 5.3.1 *Si el número real α se representa mediante una fracción continua simple periódica, entonces α es solución de una ecuación del tipo*

$$Ax^2 + Bx + C = 0 \tag{5.6}$$

con A, B y C enteros.

También se dice que α es un **irracional cuadrático**.

Demostración:

Sea

$$\alpha = [\ \overline{b_1, \ldots, b_k}\ ] = [b_1, \ldots, b_k, \alpha]$$

Entonces usando la proposición 5.2.5, se tiene

$$\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}$$

Por lo tanto α satisface una ecuación cuadrática con coeficientes enteros (Ver ejercicio 1).

II) Si α no es periódica pura, entonces

$$\alpha = [a_0, a_1, \ldots, a_n, \overline{b_1, \ldots, b_k}\ ]$$

Sea $\beta = [\ \overline{b_1, \ldots, b_k}\ ]$. Entonces por la proposición 5.2.5 se tiene

$$\alpha = [a_0, a_1, \ldots, a_n, \beta] = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}$$

Entonces es claro que, de acuerdo a la parte I, α es solución de una ecuación cuadrática del tipo (5.6).

♠

Sea α un número irracional cuadrático, entonces

$$\alpha = \frac{a + \sqrt{b}}{c}$$

donde a, b y c son enteros.

Entonces si $c > 0$, podemos multiplicar por c el numerador y denominador para obtener

$$\alpha = \frac{ac + \sqrt{bc^2}}{c^2} = \frac{m_0 + \sqrt{d}}{k_0} \tag{5.7}$$

donde k_0 divide a $m_0^2 - d$.

Teorema 5.3.1 *Sean α, m_0 y k_0 como en (5.7). Definimos*

$$\alpha_i = \frac{m_i + \sqrt{d}}{k_i}, \quad a_i = [\alpha_i],$$

donde:

$$m_{i+1} = a_i k_i - m_i, \quad k_{i+1} = \frac{d - m_{i+1}^2}{k_i}$$

Entonces k_i y m_i son enteros, para todo $i \geq 0$, k_i divide a $d - m_i^2$ y

$$\alpha = [a_0, a_1, \ldots].$$

Demostración:

En primer lugar, k_0 y m_0 están en $\mathbb{Z}$, y k_0 divide a $d - m_0^2$. Luego la proposición vale para $i = 0$. Supongamos que el resultado es cierto para un i cualquiera. Luego definimos

$$m_{i+1} = a_i k_i - m_i \in \mathbb{Z}$$

Además, podemos hacer

$$\begin{aligned} k_{i+1} &= \frac{d - (a_i k_i - m_i)^2}{k_i} \\ &= \frac{d - a_{i^2} k_i^2 + 2a_i k_i m_i - m_i^2}{k_i} \\ &= \frac{d - m_i^2}{k_i} + 2a_i m_i - a_i^2 k_i \end{aligned}$$

Luego, es claro que $k_{i+1} \in \mathbb{Z}$, por hipótesis de inducción.

Además:

$$k_i = \frac{d - m_{i+1}^2}{k_{i+1}} \in \mathbb{Z}$$

luego k_{i+1} divide a $d - m_{i+1}^2$.

Finalmente, tenemos que, para todo i

$$\begin{aligned} \alpha_i - a_i &= \frac{m_i + \sqrt{d} - a_i k_i}{k_i} \\ &= \frac{\sqrt{d} - m_{i+1}}{k_i} \\ &= \frac{d - m_{i+1}^2}{k_i\sqrt{d} + k_i m_{i+1}} \\ &= \frac{k_{i+1}}{m_{i+1} + \sqrt{d}} \\ &= \frac{1}{\alpha_{i+1}} \end{aligned}$$

Luego $\alpha = [a_0, a_1, \ldots]$.

♠

Definición 5.3.3 *Sea $x = a + b\sqrt{d}$, con a y b números racionales, entonces* **el conjugado** *de x, es el número real*

$$x' = a - b\sqrt{d}$$

Teorema 5.3.2 *Sea $\alpha = (m_0 + \sqrt{d})/k_0$ como en 5.7. Entonces α viene representado por una fracción continua simple periódica.*

Demostración:

De acuerdo a la proposición 5.2.5, se tiene

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

Sustituyendo α_n en función de α, tenemos

$$\begin{aligned}\alpha_n &= -\left(\frac{\alpha q_{n-2} - p_{n-2}}{\alpha q_{n-1} - p_{n-1}}\right) \\ &= -\frac{q_{n-2}}{q_{n-1}}\left(\frac{\alpha - \dfrac{p_{n-2}}{q_{n-2}}}{\alpha - \dfrac{p_{n-1}}{q_{n-1}}}\right)\end{aligned}$$

Tomando conjugados en ambos miembros se obtiene

$$\alpha'_n = -\frac{q_{n-2}}{q_{n-1}}\left(\frac{\alpha' - \dfrac{p_{n-2}}{q_{n-2}}}{\alpha' - \dfrac{p_{n-1}}{q_{n-1}}}\right)$$

Entonces cuando $n \to \infty$ se tiene:

$$\left(\frac{\alpha' - \dfrac{p_{n-2}}{q_{n-2}}}{\alpha' - \dfrac{p_{n-1}}{q_{n-1}}}\right) \to 1$$

Luego existe un $N > 0$ tal que $\alpha'_n < 0$, para todo $n \geq N$. Como $\alpha_n > 0$, se tiene

$$\alpha_n - \alpha'_n = \frac{2\sqrt{d}}{k_n} > 0 \quad \text{para todo } \ n \geq N.$$

Luego $k_n > 0$, y por lo tanto:

$$0 < k_{n+1}k_n = d - m_{n+1}^2 \leq d, \quad \text{para todo } \ n \geq N.$$

De esta última desigualdad se obtiene que: $0 < k_n < d$, para todo $n \geq N$. También:

$$m_{n+1}^2 < m_{n+1}^2 + k_{n+1}k_n = d$$

lo cual implica:

$$\mid m_{n+1} \mid < \sqrt{d}, \quad \text{para todo } \ n \geq N.$$

Luego las sucesiones de enteros $\{k_n\}$ y $\{m_n\}$ son finitas, y por lo tanto existe un $j > n$ tal que

$$k_n = k_j \quad y \quad m_n = m_j$$

Por lo tanto: $\alpha_n = \alpha_j$, y esto implica

$$\begin{aligned} \alpha &= [a_0, \ldots, a_{n-1}, \alpha_n] \\ &= [a_0, \ldots, a_{n-1}, a_n, \ldots, a_{j-1}, \alpha_j] \\ &= [a_0, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{j-1}}] \end{aligned}$$

Luego α es periódica. ♠

Ejemplo: Hallar la expansión de $\sqrt{7}$ como fracción continua. Sabemos que $2 < \sqrt{7} < 3$, luego $a_0 = 2$. Sea

$$\begin{aligned} r_1 &= \frac{1}{\sqrt{7}-2} \\ &= \frac{\sqrt{7}+2}{7-4} \\ &= \frac{\sqrt{7}+2}{3} \end{aligned}$$

luego $a_1 = [r_1] = 1$. De igual manera

$$\begin{aligned} r_2 &= \frac{1}{r_1 - a_1} \\ &= \frac{1}{(\sqrt{7}+2)/3 - 1} \\ &= \frac{3}{\sqrt{7}-1} \\ &= \frac{3(\sqrt{7}+1)}{6} \\ &= \frac{\sqrt{7}+1}{2} \end{aligned}$$

Luego $a_2 = [r_2] = 1$. Continuando este proceso, calculamos el siguiente a_i, para lo cual hacemos

$$\begin{aligned} r_3 &= \frac{1}{(\sqrt{7}+1)/2-1} \\ &= \frac{2}{\sqrt{7}-1} \\ &= \frac{2(\sqrt{7}+1)}{6} \\ &= \frac{\sqrt{7}+1}{3} \end{aligned}$$

por lo tanto $a_3 = [r_3] = 1$. De igual forma sea

$$\begin{aligned} r_4 &= \frac{1}{(\sqrt{7}+1)/3-1} \\ &= \frac{3}{\sqrt{7}-2} \\ &= \frac{3(\sqrt{7}+2)}{3} \\ &= \sqrt{7}+2 \end{aligned}$$

Luego $a_4 = [r_4] = 4$. Sea

$$\begin{aligned} r_5 &= \frac{1}{(\sqrt{7}+2)-4} \\ &= \frac{1}{\sqrt{7}-2} \\ &= r_1 \end{aligned}$$

Por lo tanto $a_5 = a_1 = 1$, y a partir de esta posición comienzan a repetirse los valores de a_i. Por lo tanto

$$\sqrt{7} = [\ 2, \overline{1, 1, 1, 4}\ ]$$

Ejercicios

1) Sean $\alpha = a_1 + b_1\sqrt{d}$ y $\beta = a_2 + b_2\sqrt{d}$, con a_1, a_2, b_1, b_2 números racionales. Probar:
   a) $(\alpha + \beta)' = \alpha' + \beta'$
   b) $(\alpha\beta)' = \alpha'\beta'$
   c) Para todo racional c: $(c\alpha)' = c\alpha'$.

2) Probar que si α es un irracional cuadrático, y a, b, c y d son números enteros, entonces

$$\theta = \frac{a\alpha + b}{c\alpha + d}$$

es también un irracional cuadrático.

3) Sean $\{m_i\}$, $\{k_i\}$ como en el teorema 5.3.1 Probar que existe un n, tal que:

$$m_{nj} = m_n, \quad y \quad k_{nj} = k_n, \quad \text{para todo } \ j \geq 1.$$

4) Expresar como fracción continuas los números reales:
   a) $e \cong 2.7182818$,
   b) $\pi/2$.

5) Sea $\alpha = \pi$. Hallar una fracción p/q, que no sea convergente de α y tal que:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

5.4 La Ecuación de Fermat

Consideramos ahora la ecuación

$$x^2 - dy^2 = 1$$

la cual se denomina **Ecuación de Fermat**.

Estamos interesados en hallar soluciones enteras de esta ecuación, distintas de las soluciones triviales $x = 1, x = -1, y = 0$.

Teorema 5.4.1 *Si α es un número irracional, entonces para todo $n \geq 1$ se tiene:*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n-1}} < \frac{1}{q_n^2}$$

donde p_n, q_n son las n-ésimas convergentes de α.

Demostración:

Se tiene de acuerdo a la proposición 5.2.5

$$\alpha = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}$$

donde $\alpha_n = [a_n, a_{n+1}, \ldots]$, luego $\alpha_n > 1$. Por otra parte:

$$\begin{aligned} \alpha - \frac{p_n}{q_n} &= \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{-(p_n q_{n-1} - q_n p_{n-1})}{q_n(\alpha_{n+1} q_n + q_{n-1})} \\ &= \frac{(-1)^n}{q_n(\alpha_{n+1} q_n + q_{n-1})} \end{aligned}$$

Usando $\alpha_{n+1} \geq 1$, $q_n \geq 1$ se tiene

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n-1}} < \frac{1}{q_n^2}$$

♠

Teorema 5.4.2 *Si $\dfrac{p}{q}$ es una convergente de α, entonces*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

Proposición 5.4.1 *Si* $\frac{p}{q}$ *es una convergente de* α*, entonces*

$$\alpha - \frac{p}{q} = \frac{\varepsilon\theta}{q^2} \tag{5.8}$$

donde $\varepsilon = \pm 1,\ \ 0 < \theta < 1$.

Observación: Si p/q es una fracción que satisface (5.8) entonces no se puede afirmar que p/q sea una convergente de α. Sin embargo, es posible dar una condición adicional, como veremos más adelante, de tal forma que se tenga un resultado recíproco del teorema anterior.

La siguiente condición se debe a Legendre:

Teorema 5.4.3 *Sea* α *un número irracional. Si* $\frac{p}{q}$ *es un número racional tal que*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

entonces $\frac{p}{q}$ *es una convergente de* α.

Demostración:

Sea

$$\frac{p}{q} = [a_0, a_1, \ldots, a_n]$$

De la hipótesis se deduce que

$$\alpha - \frac{p}{q} = \frac{\varepsilon\theta}{q^2}$$

con $\varepsilon = \pm 1$, y $0 < \theta < 1/2$.

Entonces podemos elegir n, sin pérdida de generalidad, de tal forma que $\varepsilon = (-1)^n$.

Definamos el número racional β mediante la fórmula

$$\alpha = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}$$

Entonces

$$\begin{aligned} \frac{p}{q} - \alpha &= \frac{p_n}{q_n} - \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}} \\ &= \frac{p_n q_{n-1} - q_n p_{n-1}}{q_n(\beta q_n + q_{n-1})} \\ &= \frac{(-1)^n}{q_n(\beta q_n + q_{n-1})} \end{aligned}$$

Si resolvemos esta ecuación para β tendremos

$$\beta = \frac{q_n - \theta q_{n-1}}{q_n \theta}$$

De donde se deduce $\beta > 1$, pues $0 < \theta < 1/2$ y $q_{n-1} < q_n$.

Podemos entonces representar a β como una fracción continua

$$\beta = [a_{n+1}, \ldots]$$

luego definimos:

$$\begin{aligned} \gamma &= [a_0, a_1, \ldots, a_n, a_{n+1}, \ldots] \\ &= [a_0, \ldots, a_n, \beta] \end{aligned}$$

Luego

$$\gamma = \frac{p_n \beta + p_{n-1}}{q_n \beta + q_{n-1}} = \alpha$$

Por lo tanto $p/q = p_n/q_n$ es una convergente de α. ♠

Teorema 5.4.4 *Sea* $\alpha = \sqrt{d}$ *y*

$$\alpha_n = \frac{m_n + \sqrt{d}}{k_n}$$

entonces la ecuación

$$x^2 - dy^2 = (-1)^n k_n$$

posee solución.

Demostración:

Usando la proposición 5.2.5 se obtiene:

$$\begin{aligned} \sqrt{d} &= \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} \\ &= \frac{(\sqrt{d} + m_n)p_{n-1} + p_{n-2}k_n}{(\sqrt{d} + m_n)q_{n-1} + q_{n-2}k_n} \end{aligned}$$

de donde:

$$\sqrt{d}\left\{(\sqrt{d} + m_n)q_{n-1} + q_{n-2}k_n\right\} = (\sqrt{d} + m_n)p_{n-1} + p_{n-2}k_n$$

Igualando coeficientes racionales e irracionales nos da:

$$p_{n-1} = m_n q_{n-1} + k_n q_{n-2} \tag{5.9}$$

$$dq_{n-1} = m_n p_{n-1} + k_n p_{n-2} \tag{5.10}$$

Multiplicando la primera ecuación por p_{n-1}, la segunda por q_{n-1} y luego restando nos da

$$\begin{aligned} p_{n-1}^2 - dq_{n-1}^2 &= k_n(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) \\ &= (-1)^n k_n. \end{aligned}$$

♠

Proposición 5.4.2 *Sea n el período de $\sqrt{d}$ como fracción continua. Entonces $k_n = 1$*

Demostración:

Sea

$$\alpha = \alpha_0 = \frac{m_0 + \sqrt{d}}{k_0}$$

Entonces $m_0 = 1$ y $k_0 = 1$ De acuerdo a la definición de período, se debe cumplir:

$$\alpha_n = \frac{m_n + \sqrt{d}}{k_n} = \sqrt{d}$$

por lo tanto:

$$(k_n - 1)\sqrt{d} = m_n$$

de donde se obtiene $k_n = 1$. ♠

Teorema 5.4.5 *Sea d un entero positivo libre de cuadrados, entonces la ecuación:*

$$x^2 - dy^2 = 1$$

posee infinitas soluciones

Demostración:

Nuevamente, sea n el período de la descomposición de $\sqrt{d}$ en fracción continua.

Si n es par, tomamos:

$$x = p_{nj-1} \quad y = q_{nj-1}$$

donde j es cualquier entero positivo. En virtud de la proposición anterior se tiene:

$$(p_{nj-1})^2 - (q_{nj-1})^2 d = (-1)^{nj} k_{nj} = 1.$$

Si n es impar, tomamos

$$x = p_{2nj-1} \quad y = q_{2nj-1}$$

Luego:

$$(p_{2nj-1})^2 - d(q_{2nj-1})^2 = (-1)^{2nj} k_{2nj} = 1$$

♠

Ejemplo:
Resolver:

$$x^2 - 7y^2 = 1$$

Solución:

Hemos visto que la expansión de $\sqrt{7}$ en fracción continua viene dada por:

$$\sqrt{7} = [2, \overline{1, 1, 1, 4}\ ]$$

Podemos usar el algoritmo dado al comienzo para calcular las convergentes. Esto lo expresamos mediante la siguiente tabla:

n	a_{n+1}	p_n	q_n
0	1	2	1
1	1	3	1
2	1	5	2
3	4	8	3
4	1	37	14
5	1	45	17
6	1	82	31
7	1	127	48

Vemos que $(8, 3)$ es solución , al igual que $(127, 48)$. Podemos continuar generando más soluciones por intermedio de la tabla. Claramente, ellas aparecen entre las convergentes con un período de 4.

Teorema 5.4.6 *Si el par (p, q) es una solución de*

$$x^2 - dy^2 = 1$$

con $d \geq 5$, entonces la fracción p/q es una convergente de $\sqrt{d}$.

Demostración:

Tenemos:

$$\begin{aligned} p^2 - dq^2 &= (p - \sqrt{d}q)(p + \sqrt{d}q) \\ &= 1. \end{aligned}$$

Luego:

$$\begin{aligned} \left| \frac{p}{q} - \sqrt{d} \right| &= \frac{1}{q(p + \sqrt{d}q)} \\ &< \frac{1}{q^2\sqrt{d}} \\ &< \frac{1}{2q^2} \end{aligned}$$

Luego por el teorema, concluimos que p/q es una convergente de $\sqrt{d}$.

♠

Ejercicios

1) Resolver

$$x^2 - 11y^2 = 1$$

2) En la ecuación de Fermat

$$x^2 - y^2 = 1,$$

el lado izquierdo se puede factorizar

$$x^2 - y^2 = (x + iy)(x - iy).$$

Los números complejos de la forma $x + iy$ se denominan **enteros de Gauss**

a) Investigue todo lo concerniente a los enteros de Gauss.
b) Resuelva la ecuación dada.

3) Sean x_1, y_1, x_2, y_2 números enteros. Probar la identidad

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2$$

4) Usando la identidad anterior, probar que si (x_1, y_1) y (x_2, y_2) son ambos solución de la ecuación

$$x^2 - dy^2 = 1$$

entonces también lo es (x_3, y_3), donde

$$x_3 = x_1x_2 - dy_1y_2, \quad y_3 = x_1y_2 - y_1x_2.$$

5) Resolver:
a) $x^2 - 3y^2 = 1$
b) $x^2 - 15y^2 = 1$
c) $x^2 - 6y^2 = -1$

6) Investigue bajo que condiciones sobre f y d se puede resolver

$$x^2 - dy^2 = f$$

Bibliografía

[1] Bravo Flores, Raúl - *Fundamentos de los sistemas numéricos* Editorial Interamericana . México- 1971.

[2] W.W.Adams and L.J.Goldstein - *Introduction to number theory* Englewood Cliffs, N.J. Prentice-Hall 1976

[3] R. Ayoub- "Euler and the zeta function". Am. Math. Monthly, 81 (1974) p. 1067-1086

[4] Carl Boyer - *A History of Mathematics.* John Wiley and son - New York 1968.

[5] Lucas N.H. Bunt, Phillip S. Jones - *The historical roots of elementary mathematics.* Dover 1976, New York.

[6] Lindsay Childs - *A concrete introduction to Higher Algebra.* Springer Verlag New York 1979.

[7] C.H. Cleminshaw - "The Julian Period". The Griffith Observer April 1975.

[8] David A. Cox - "Introduction to Fermat's Last Theorem". Amer.Math. Monthly - Jan. 1994.

[9] Heinrich Dörrie - *100 Great Problems of Elementary Mathematics.* Dover Publications INC. New York 1965.

[10] J. E. Hofmann - *Pierre de Fermat.* Dictionary of Scientific Biography.

[11] Carl Friedrich Gauss- *Disquisitiones Arithmeticae.* Traducida por Arthur A. Clarke New Haven and London, Yale University Press, 1966.

[12] L. J. Goldstein - "A history of the prime number theorem". Am. Math. Monthly, 80 (1973), p. 599- 615.

[13] Thomas Heath - *A history of greek mathematics.*
Dover Pub. Inc, New York 1981.

[14] I.N. Herstein - *Topics in Algebra.*
John Wiley and son New York, 1975.

[15] K. Ireland and M. Rosen - *A classical introduction to Modern Number Theory.*
Springer Verlag, New York - 1982.

[16] J. Itard -*Joseph Louis Lagrange.*
Dictionary of Scientific Biography.

[17] Y. Itard -*Adrien Marie Legendre.*
Dictionary of Scientific Biography.

[18] K. O. May - *C. F. Gauss.*
Dictionary of Scientific Biography.

[19] B. Mazur - "Number Theory as gadfly".
Amer. Math. Monthly (1991) vol 88, p.593-610.

[20] Gordon Moyer - "The origin of the Julian Day System".
Sky and Telescope April 1981.

[21] O. Neugebauer - *A history of Ancient Mathematical Astronomy.*
Springer Verlag Berlin 1975.

[22] I. Niven, H. S. Zuckerman - *Introduction to Number Theory.*
New York, Wiley 1966.

[23] Ho Peng-Yoke - *Ch'in Chiu- Shiao.*
Dictionary of Scientific Biography.

[24] P. Ribenboim - 13 *Lectures on Fermat's Last Theorem.*
Springer Verlag, New York 1979.

[25] Ronald Reese, Steven Everet - "J. J. Scaliger and the Julian Period".
The Griffith Observer, May 1981.

[26] Ronald Reese, Steven Everet - "The origin of the Julian Period". Am. J. Phys 49 (7) , July 1981.

[27] Winfried Scharlau, Hans Opolka -*From Fermat to Minkowsky.* Springer Verlag- New York - 1985.

[28] D. E. Smith - *History of Mathematics.* Dover, New York 1958.

[29] Toomen G. J. - *Al- Khowarizmi.* Dictionary of Scientific Biography .

[30] H.S.Vandiver - "Fermat's Last Theorem". Amer.Math.Monthly 53 (1946) 555- 578.

[31] A. Youschkevitch, B.A.Rosefeld - *Al- Kashi.* Dictionary of Scientific Biography.

[32] A. Youschkevitch - *Leonhard Euler.* Dictionary of Scientific Biography.