UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMÁTICA

SECCIÓN MATEMÁTICA

TRABAJO DE GRADUACIÓN:

“LA LEY DE RECIPROCIDAD.”

PRESENTAN:

ARGUETA PORTILLO, SANDRA PATRICIA.

SARAVIA MÁRQUEZ, WALTER ANTONIO.

PARA OPTAR AL TITULO DE:

LICENCIADO EN MATEMÁTICA.

MARZO DE 2015

SAN MIGUEL, EL SALVADOR CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR.

RECTOR: Ing. Mario Roberto Nieto Lovo.

VICERRECTORA ACADEMICA: Maestra Ana María Glower de Alvarado.

VICERRECTOR ADMINISTRATIVO: Lic. Salvador Castillo.

SECRETARIA GENERAL: Dra. Ana Leticia de Amaya.

FACULTAD MULTIDISCIPLINARIA ORIENTAL.

DECANO: Lic. Cristóbal Hernán Ríos Benítez.

VICEDECANO: Lic. Carlos Alexander Díaz.

ADMINISTRACION ACADEMICA: Lic. Jeovanny Trejos Cabrera.

DEPARTAMENTO DE CIENCIAS NATURALES Y MATEMATICA.

JEFE: Lic. José Enry García.

SECCION DE MATEMATICA.

COORDINADOR: Ing. Benedicto Saravia.

TRABAJO DE GRADUACION APROBADO POR:

_____

Msc. Oscar Ulises Lizama Vigil.

Coordinador de Procesos de Graduación

Depto. de Ciencias Naturales y Matemática

_____

Licda. Sonia del Carmen Martínez de López

Asesor Director

AGRADECIMIENTOS.

Walter Antonio Saravia Márquez:

A **Dios**, por darme salud, fortaleza, sabiduría y protección; a mi **madre** por haberme apoyado en cada momento, por su confianza, cariño y soportar tantos momentos difíciles; a mi **hermano** por comprenderme durante mis ausencias y apoyarme cuando lo necesité.

A mi novia **Johanna** por siempre estar conmigo y por su amor.

A mis **tías, tíos y a mi abuela** por su amor incondicional y al recuerdo de los que ya no están entre nosotros y que tuve la oportunidad de recibir su amor.

A mis **amigos** que me brindaron su amistad y cariño y a los que de alguna forma formaron parte de mi vida.

A mi compañera de tésis **Sandra Patricia Argueta Portillo** por su trabajo arduo y dedicación.

Y en especial a las personas que aportaron a mi formación académica **Licda. María del Tránsito Gutiérrez**, **MSc. Jorge Alberto Martínez, Licda. María Olga Quintanilla de Lovo y Licda. Sonia del Carmen Martínez de López,** gracias por siempre apoyarme y nunca negarme la ayuda cuando la necesité y por enseñarme y guiarme en el trayecto de mi carrera y más en mi vida.

Sandra Patricia Argueta Portillo:

Primeramente agradecer especialmente a **Dios** por haberme permitido llegar a este momento tan especial en mi vida, por darme salud y sabiduría.

A mi **madre Cristina Portillo** por su amor y porque a pesar de las dificultades siempre conté con su apoyo, sus consejos y su confianza. A mi **padre Florentín Argueta** por sus sacrificios, por haberme apoyado incondicionalmente y a mis **hermanos** por ayudarme cuando más los necesite.

A toda **mi familia** porque de una u otra forma siempre conté con su ayuda. A **mis compañeros** por brindarme su amistad. A mi compañero de tésis **Walter Antonio Saravia Márquez**.

De manera especial agradezco a todos los docentes que aportaron a mi formación académica a mi **profesor Ezequías Solórzano** que formó parte esencial en mi educación al **MSc. Jorge Alberto Martínez**, **Licda. María Olga Quintanilla de Lovo** y **Licda. Sonia del Carmen Martínez de López**, por su ayuda.

INDICE

INTRODUCCIÓN

Matemática proviene del latín mathematĭca, aunque con origen más remoto en un vocablo griego que puede traducirse como “conocimiento”, la matemática es la ciencia deductiva que se dedica al estudio de las propiedades de los entes abstractos y de sus relaciones. A partir de axiomas y siguiendo razonamientos lógicos, la matemática analiza estructuras, magnitudes y vínculos de los entes abstractos. Esto permite, una vez detectados ciertos patrones, formular conjeturas y establecer definiciones a las que se llegan por deducción. Esto quiere decir que la matemática trabaja con números, símbolos, figuras geométricas, etc.

La teoría elemental de números, es una de las ramas de la Matemática en donde se estudian los números enteros sin emplear técnicas procedentes de otros campos de la matemática. Pertenecen a la teoría elemental de números las cuestiones de divisibilidad, el algoritmo de Euclides utilizado para calcular el máximo común divisor, la factorización de los enteros como producto de números primos, la búsqueda de los números perfectos y las congruencias, entre otros. Son enunciados típicos el pequeño teorema de Fermat y el teorema de Euler que lo extiende, el teorema chino del resto y la ley de reciprocidad cuadrática.

La ley de reciprocidad cuadrática es uno de los resultados más útiles dentro de esta rama. Desde que fue enunciada (explícitamente) en 1772 por Euler ha sido materia

de estudio de numerosos personajes. Se puede afirmar que la teoría de números moderna comenzó con el descubrimiento de la ley de reciprocidad cuadrática.

El primer capítulo está constituido por todas aquellas definiciones preliminares que nos serán de utilidad en el transcurso de este trabajo, en primer lugar abordaremos un poco sobre la historia de la teoría de números que remota desde tiempos antiguos así como el avance que esta ha tenido hasta los últimos años, luego introduciremos desde la definición de números enteros hasta la determinación de números primos.

En el segundo capítulo tratamos sobre todo lo relacionado con la teoría de congruencias es decir las definiciones, teoremas, lemas y corolarios, tratando de manera especial el teorema chino del residuo.

En el tercer capítulo abordamos la demostración de la ley de reciprocidad cuadrática, como un caso especial desarrollaremos de la primera demostración de la ley de reciprocidad cuadrática la cual fue realizada por Gauss y plantearemos también algunos ejemplos para observar el funcionamiento y la importancia de esta ley.

ANTECEDENTES

Haciendo un recorrido por la historia de la matemática y teniendo a la Ley de Reciprocidad Cuadrática como eje central, el primero que ofrece de manera implícita una parte de la primera ley complementaria de la Ley de Reciprocidad Cuadrática es Diofanto de Alejandría, en su obra Arithmetica. Luego, Fermat motivado por este libro encuentra parte esencial de la primera ley complementaria de la Ley de Reciprocidad Cuadrática: como lo expresa en una carta a su amigo Mersenne en 1640. Fue Kronecker, quien en 1875 sugirió el hecho de que la Ley de Reciprocidad Cuadrática había sido ya expuesta por Euler en 1783, quien se inició en el estudio de esta ley gracias al trabajo antes realizado por Fermat. Euler encuentra entre 1741 y 1742 la primera forma implícita de la Ley de Reciprocidad Cuadrática y posteriormente en 1772 consigue la segunda o forma explícita de la Ley de Reciprocidad Cuadrática, publicada después de su muerte en Opúscula Analítica de 1783. Cabe notar ahora que ninguno de estos matemáticos demostró la Ley de Reciprocidad Cuadrática; posteriormente sólo Legendre ofreció una prueba parcial de dicho teorema.

Fue en 1796 cuando Carl Friederich Gauss realizó la primera demostración completa de la Ley de reciprocidad Cuadrática publicándola posteriormente en su magna obra Disquisitiones Arithmeticae. A lo largo de su vida Gauss realizó ocho demostraciones de esta ley que él denominó Theorema Aureum (Teorema Aureo). Es importante resaltar que las demostraciones de Gauss sirvieron de impulso para que otros grandes matemáticos se dieran a la tarea de desarrollar teorías tan

importantes como la Teoría Algebraica de Números y que otros encaminaran sus esfuerzos en trabajos paralelos a este.

JUSTIFICACIÓN

Debido a la importancia que la Ley de Reciprocidad Cuadrática tiene en la matemática, especialmente en el área de Teoría del Número se tiene la necesidad de conocer más sobre él, es por eso que esta investigación bibliográfica se realiza con el objetivo de estudiar y presentar dicha ley. Cabe destacar que La Ley de Reciprocidad Cuadrática ha servido de base para la obtención de otros resultados interesantes en diversos campos de la matemática.

Por medio de la Ley de Reciprocidad Cuadrática, se pueden determinar si existen soluciones o no, de una ecuación cuadrática del tipo:

$$x^2 \equiv a \ (mod\ p)$$, donde p es primo y $mcd(a,p) = 1$.

El trabajo de investigación es de mucho interés; los contenidos de este se desarrollarán con una secuencia lógica para mayor comprensión del tema, de tal manera que este pueda ser entendido y asimilado fácilmente, por lo que se partirá desde los conceptos básicos además, presentaremos los teoremas, lemas, corolarios y propiedades que nos servirán como base para luego enunciar la Ley de Reciprocidad Cuadrática.

Así mismo, con esta investigación se pretende que para las personas a quienes interese el área de Teoría del Número y desean conocer sobre este tema, sea de utilidad y con ello se tenga una mayor información del tema de investigación.

OBJETIVOS

3.1 Objetivo General:

- Presentar la Ley de Reciprocidad Cuadrática y dar a conocer mediante ejemplos el funcionamiento y la importancia de ésta en la Teoría Elemental de Números.

3.2 Objetivos Específicos:

- Mostrar conceptos básicos de la Teoría Elemental de Números.

- Presentar la primera demostración de La Ley de Reciprocidad Cuadrática.

- Dar a conocer mediante ejemplos la aplicación, el funcionamiento y la importancia de la Ley de Reciprocidad Cuadrática en la Teoría Elemental de Números.

CAPITULO I

PRELIMINARES

1.1. Historia.

La historia de Teoría del Número es bastante extensa, tan larga como la del hombre y nos enseña como 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.

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.

1.1.1. Época Antigua

El origen de la Teoría del Número 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 de la ecuación

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

Como por ejemplo el triplete $(3, 4, 5)$, el cual satisface: $3^2 + 4^2 = 5^2$. Los babilónicos conocían esta y otras soluciones, nos dejaron una lista de más de setenta 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, una muestra de la capacidad de razonamiento abstracto de los matemáticos griegos son todos esos teoremas aportados a la matemática. Así vemos como Pitágoras 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 del Número es muy importante.

El primero de ellos es Euclides, quien establece una serie de proposiciones sobre los números enteros, las cuales pueden ser consideradas como el inicio de la Teoría del Número. Por ejemplo la prueba de que existe un número infinito de números primos. También a Euclides se debe el algoritmo para hallar el máximo común divisor entre dos enteros.

El segundo es Diofanto de Alejandría, cuya contribución a la Teoría del Número ha sido fundamental, es llamado también el Padre de la Teoría del Número. Diofanto escribió muchos libros de matemática, además conocía algunos hechos importantes de la Teoría del Número. Otro aporte importante fue el estudio de los números poligonales (un número es poligonal cuando representa la suma de los puntos enteros dentro de un polígono). La obra de Diofanto ciertamente dio inicio a la Teoría del Número. Sin embargo no fue apreciada en toda su magnitud por los

matemáticos posteriores. Transcurrieron varios siglos sin haber algún hecho importante en esta área de la matemática

1.1.2. Época Moderna.

Iniciando la nueva era de la matemática moderna, encontramos la figura de Pierre de Fermat, uno de los más grandes matemáticos en el área de Teoría del Número, estudió profundamente la obra de Diofanto, 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 del Número, pues Fermat pudo hallar soluciones muy generales para muchas ecuaciones Diofánticas, usando métodos de demostración suficientemente rigurosos.

El interés de Fermat por la Teoría del Número 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. 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 del Número a manera de reto.

La intuición de Fermat para plantear problemas en Teoría del Número, es realmente maravillosa. Algunos de estos problemas los resolvió usando sus propias técnicas, otros, sin embargo, fueron resueltos por matemáticos de siglos posteriores.

Es importante destacar la labor realizada por Euler, quien continuó la obra de Fermat, resolviendo algunos problemas difíciles planteados por Fermat. En el

campo de la Teoría del Número, Euler inició una nueva etapa es esta área, al probar algunos teoremas usando métodos del análisis.

Lagrange expone ante la Real Academia uno de sus mejores resultados en Teoría del Número: 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.

Uno de los matemáticos contemporáneos de Lagrange, cuya obra tuvo mucha influencia en el desarrollo posterior de la Teoría del Número, fue Adrien-Marie Legendre. En 1798 publicó una obra titulada: Ensayo sobre la Teoría del Número 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.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.

1.2. Biografías.

1.2.1. Karl Friedrich Gauss

(Brunswick, actual Alemania, 1777 - Gotinga, id., 1855) Matemático, físico y astrónomo alemán. Nacido en el seno de una familia humilde, desde muy temprana edad Karl Friedrich Gauss dio muestras de una prodigiosa capacidad para las matemáticas (según la leyenda, a los tres años interrumpió a su padre cuando estaba ocupado en la contabilidad de su negocio para indicarle un error de cálculo), hasta el punto de ser recomendado al duque de Brunswick por sus profesores de la escuela primaria.

El duque le proporcionó asistencia financiera en sus estudios secundarios y universitarios, que efectuó en la Universidad de Gotinga entre 1795 y 1798. Su tesis doctoral (1799) versó sobre el teorema fundamental del álgebra (que establece que toda ecuación algebraica de coeficientes complejos tiene soluciones igualmente complejas), que Gauss demostró.

En 1801 Gauss publicó una obra destinada a influir de forma decisiva en la conformación de la matemática del resto del siglo, y particularmente en el ámbito de la Teoría del Número, las Disquisiciones aritméticas, su obra más famosa, en donde Gauss sienta las bases de la Teoría del Número, como una de la disciplinas más sólidas y ricas de la matemática; entre cuyos numerosos hallazgos cabe destacar: la primera prueba de la ley de la reciprocidad cuadrática; una solución algebraica al problema de cómo determinar si un polígono regular de n lados puede ser construido de manera geométrica (sin resolver desde los tiempos de Euclides); un

tratamiento exhaustivo de la teoría de los números congruentes; y numerosos resultados con números y funciones de variable compleja que marcaron el punto de partida de la moderna teoría de los números algebraicos.

.

Su fama como matemático creció considerablemente ese mismo año, cuando fue capaz de predecir con exactitud el comportamiento orbital del asteroide Ceres, avistado por primera vez pocos meses antes, para lo cual empleó el método de los mínimos cuadrados, desarrollado por él mismo en 1794 y aún hoy día la base computacional de modernas herramientas de estimación astronómica.

En 1807 aceptó el puesto de profesor de astronomía en el Observatorio de Gotinga, cargo en el que permaneció toda su vida. Dos años más tarde, su primera esposa, con quien había contraído matrimonio en 1805, falleció al dar a luz a su tercer hijo; más tarde se casó en segundas nupcias y tuvo tres hijos más. En esos años Gauss maduró sus ideas sobre geometría no euclidiana, esto es, la construcción de una geometría lógicamente coherente que prescindiera del postulado de Euclides de las paralelas; aunque no publicó sus conclusiones, se adelantó en más de treinta años a los trabajos posteriores de Lobachewski y Bolyai.

Alrededor de 1820, ocupado en la correcta determinación matemática de la forma y el tamaño del globo terráqueo, Gauss desarrolló numerosas herramientas para el tratamiento de los datos observacionales, entre las cuales destaca la curva de distribución de errores que lleva su nombre, conocida también con el apelativo de distribución normal y que constituye uno de los pilares de la estadística.

1.2.2. Pierre de Fermat

(Beaumont, Francia, 1601 - Castres, id., 1665) Matemático francés.

Fermat nació el mismo año que el siglo XVII y aunque sus contribuciones matemáticas nunca fueron publicadas en vida, fueron de tal calidad que la difusión que tuvieron entre la comunidad científica europea fue suficiente como para que su siglo le recuerde como uno de sus mejores hijos. Y eso que el diecisiete fue un siglo pródigo en matemáticos y científicos de primera fila. Poco se conoce de sus primeros años, excepto que estudió derecho, posiblemente en Toulouse y Burdeos. Interesado por las matemáticas, en 1629 abordó la tarea de reconstruir algunas de las demostraciones perdidas del matemático griego Apolonio relativas a los lugares geométricos; a tal efecto desarrollaría, contemporánea e independientemente de René Descartes, un método algebraico para tratar cuestiones de geometría por medio de un sistema de coordenadas.

Otro campo en el que realizó destacadas aportaciones fue el de la Teoría del Número, en la que empezó a interesarse tras consultar una edición de la Aritmética de Diofanto; precisamente en el margen de una página de dicha edición fue donde anotó el célebre teorema que lleva su nombre y que tardaría más de tres siglos en demostrarse. De su trabajo en dicho campo se derivaron importantes resultados relacionados con las propiedades de los números primos, muchas de las cuales quedaron expresadas en forma de simples proposiciones y teoremas.

Desarrolló también un ingenioso método de demostración que denominó «del descenso infinito». Extremadamente prolífico, sus deberes profesionales y su

particular forma de trabajar (sólo publicó una obra científica en vida) redujeron en gran medida el impacto de su obra.

Pero el tema que ha de dar a Fermat fama universal es el de Teoría del Número. Su interés por los números enteros y sus maravillosas propiedades había empezado en la década de los 1630 cuando Fermat leyó la traducción de Bachet de la Aritmética de Diofanto. El enorme interés de Fermat por los números enteros era una novedad en la Europa del siglo XVII. Nadie tenía demasiado interés en perder el tiempo explorando propiedades de números enteros que no tenían ninguna aplicación directa. Sólo un par de problemas clásicos atraían la atención de los matemáticos de la época: el estudio de números perfectos (aquellos que son iguales a la suma de sus divisores, exceptuando ellos mismos) y la caracterización de las ternas pitagóricas (tripletes de números enteros (x, y, z) que satisfacen el teorema de Pitágoras). Como consecuencia del interés de Fermat en el primero de esos problemas, Fermat descubrió el que se conoce hoy en día como el Pequeño Teorema de Fermat, una verdadera joya en Teoría del Número.

1.3. Números Enteros.

Dedicamos este apartado al estudio de los números enteros los cuales son el punto de partida de la Teoría del Número. Estudiaremos algunas de las propiedades básicas de este conjunto.

Definición 1.3.1

Los números enteros son un conjunto de números que incluye a los números naturales distintos de cero $\{1, 2, 3, \dots\}$, los negativos de los números naturales $\{\dots, -3, -2, -1\}$ y al 0. Los enteros negativos, como −1 o −3 (se leen «menos uno», «menos tres», etc.), son menores que todos los enteros positivos $\{1, 2, 3, \dots\}$ y que el cero. La notación de los números enteros está dada por:

$$\mathbb{Z} = \{\dots -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}.$$

Los números enteros son el ingrediente principal en Teoría del Número la cual está relacionada primordialmente con las propiedades de los números naturales, 1, 2, 3,… también llamados enteros positivos. Sin embargo, la Teoría del Número no se limita estrictamente a los números naturales ni aun al conjunto de todos los enteros ±1, ±2, ±3,…. de hecho algunos teoremas de Teoría del Número se prueban más fácilmente haciendo uso de las propiedades de los números reales.

Establecemos algunas de las propiedades de los números enteros:

1.3.2 Propiedades de los números enteros

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 numero entero.

2. **Conmutativa.**

   Para a y b números enteros, $a + b = b + a$.

3. **Asociativa.**

   Para a, b y c números enteros, $(a + b) + c = a + (b + c)$.

4. **Elemento neutro.**

   Existe un elemento en $\mathbb{Z}$ llamado el cero, el cual se denota por 0, y para todo a entero satisface:

   $$0 + a = a + 0 = a.$$

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

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

Y

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

Definición 1.3.3

Una relación de orden en un conjunto A, es una relación binaria 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 $a = b$.

Definición 1.3.4 (Axiomas de Orden).

Existe un conjunto de enteros, llamados enteros positivos, el cual denotaremos por $\mathbb{N}$, y que satisface:

1. Para todos a y b en $\mathbb{N}$, $a + b$ y $a \cdot b$ están en $\mathbb{N}$.
2. 1 está en $\mathbb{N}$.
3. Ley de tricotomía.

Para todo entero a se tiene una y sólo una de las siguientes proposiciones:

i) a está en $\mathbb{N}$, ii) $-a$ está en $\mathbb{N}$, iii) $a = 0$.

Definición 1.3.5 (Principio del Buen Orden)

Todo conjunto no vacío S de números enteros positivos contiene un elemento mínimo; esto es existe un entero a en S tal que $a \leq b$ para todo b que pertenece a S.

Definición 1.3.6 (Valor absoluto)

Definimos el valor absoluto o módulo de todo número entero a como

$$|a| = \begin{cases} a, & si\ a \geq 0 \\ -a & si\ a < 0 \end{cases}$$

Por definición, el valor absoluto de a, siempre será mayor o igual que cero y nunca negativo.

Ejemplo 1:

$|1| = 1, |-4| = -(-4) = 4$

Teorema 1.3.7 (Algoritmo de la división)

Sea a un entero positivo y b un entero arbitrario. Entonces existen los enteros q y r únicos, tales que:

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

Demostración.

Primero vamos a demostrar 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

$$D = \{b - ua \ / \ u \ es \ un \ entero\}.$$

Este conjunto contiene enteros positivos.

Si $b > 0$, basta tomar $u = 0$.

Si por el contrario $b < 0$, hacemos $u = b$, con lo cual

$$b - ba > 0, \qquad \text{y} \qquad b - ba \in D.$$

Por lo tanto el conjunto D es diferente de vacío.

Por la definición del mínimo elemento, este conjunto posee un elemento mínimo r el cual pertenece a D.

Luego, existe un entero q, tal que

$$r = b - qa, \qquad \text{o bien} \qquad b = qa + r, \quad 0 \leq r.$$

Si suponemos que

$$r \geq a$$

Se tiene que

$$r - a \geq 0$$

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.

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

$$b = \mathrm{q}a + \mathrm{r}, \qquad 0 \leq \mathrm{r} < a.$$
$$b = q'a + r', \qquad 0 \leq r' < a.$$

Entonces,

$$qa + \mathrm{r} = q'a + r'$$
$$\Longrightarrow (q - q')a = r' - r$$
$$\Longrightarrow |q - q'|a = |r' - r|$$

Además sabemos que

$$0 \leq r', \qquad r < a.$$

Entonces

$$0 \leq |r' - r| < a.$$

Luego tenemos

$$\left.\begin{matrix} |q - q'|a = |r' - r| \\ |r' - r| < a \end{matrix}\right\} \Longrightarrow |q - q'|a < a$$

$$\Longrightarrow -a|q - q'| > -a$$

$$\Longrightarrow a - a|q - q'| > 0$$

$$\Longrightarrow a(1 - |q - q'|) > 0.$$

Al ser $a > 0,$ tendremos que

$$1 - |q - q'| > 0.$$

De donde se sigue que

$$0 \leq |q - q'| < 1.$$

Y como q y q' son enteros, se tiene

$$|q - q'| = 0.$$

Por lo tanto

$$q = q',$$

y

$$r' = r. \quad \blacksquare$$

Definición 1.3.8 (Divisibilidad)

Se dice que un número entero b es divisible entre un entero a o que b es exactamente divisible por $a,$ con a distinto de cero, si existe un entero c tal que:

$b = a\,.\,c$ y se denota por $a\,/\,b$. En el caso en que b no sea divisible por a se escribe $a \nmid b$.

Naturalmente, todo número entero a distinto de 1 y -1 tiene, al menos, cuatro divisores, a saber ± 1 y $\pm a$. A estos divisores se les conoce con el nombre de divisores triviales de a.

Ejemplo 2:

18 es divisible por 3 ya que 18=6(3).

Teorema 1.3.9

Sean a, b, c, d, p y q enteros. Entonces

1. $a \mid 0, \quad 1 \mid a, \quad a \mid a$.
2. $a \mid 1$ si y solo si $a = \pm 1$.
3. Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.
4. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
5. $a \mid b$ y $b \mid a$ entonces $|a| = |b|$.
6. Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$.
7. Si $a \mid b$ y $a \mid c$, entonces $a \mid (bx + cy)$ para x e y enteros arbitrarios.
8. Si $a \mid (p + q)$ y $a \mid p$ entonces $a \mid q$.
9. Si $a \mid b$, entonces $a \mid mb$, para todo $m \in \mathbb{Z}$.

Demostración.

1. $a/0,\ \ 1/a,\ \ a/a.$

   Sea $0 = a \cdot c$ si $c = 0$ se cumple para todo a.

   Sea $a = 1 \cdot c$ si $c = a$ se cumple para todo a.

   Sea $a = a \cdot c$ si $c = 1$ se cumple para todo a.

2. $a \,/\, 1$ si y solo si $a = \pm 1$.

   "$\Longrightarrow$" $a|1$ entonces $a = \pm 1$

   Por hipótesis

   $$a|1$$

   Entonces

   $$1 = a \cdot c,$$

   lo cual es posible solo si

   $$c = 1 \ y \ a = 1 \qquad \text{o} \qquad c = -1 \ y \ a = -1.$$

   Luego $a = \pm 1.$

   "$\Longleftarrow$" si $a = \pm 1$ entonces $a \,/\, 1.$

   Si $a = 1$, entonces

   $1 = (1)(1) = a \cdot (1),$ Sustituyendo $a = 1.$

   Luego $a \,/\, 1.$

   Si $a = -1$, entonces

   $1 = (-1)(-1) = a \cdot (-1),$ Sustituyendo $a = -1.$

Luego $a \mid 1$.

3. Si $a \mid b$ y c/d, entonces ac/bd.

   Sea $b = na$ y $d = mc$.

   Entonces

   $$bd = (na)(mc)$$

   $$bd = (nm)(ac).$$

   De donde

   $$ac/bd.$$

4. Si $a \mid b$ y b/c, entonces a/c.

   Sea $b = na$ y $c = mb$.

   Entonces

   $$c = m(na)$$

   $$c = (mn)a.$$

   De donde

   $$a/c.$$

5. Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$.

   Sea $b = na$.

Como $b \neq 0$, implica que $n \neq 0$. Obteniendo el valor absoluto de ambos lados tenemos

$|b| = |na| = |n||a|$.

Como $n \neq 0$ entonces $n \geq 1$.

De donde

$$|b| = |n||a| \geq |a|.$$

6. $a \mid b$ y b/a entonces $|a| = |b|$.

   Si $a \mid b$ y b/a, entonces por definición de divisibilidad $b \neq 0$ y $a \neq 0$, entonces por el numeral 5) tenemos que

   $|b| \geq |a| \quad y \quad |a| \geq |b|$,

   por lo tanto

   $$|a| = |b|$$

7. Si a/b y a/c, entonces $a \mid (bx + cy)$ para x e y enteros arbitrarios.

   Sea $b = ac$ y $c = am$,

   entonces

   $$bx + cy = acx + amy$$

   $$bx + cy = (cx + my)a$$

De donde

$$a/(bx + cy).$$

8. Si $a \,/\, (p + q)$ y $a \,/\, p$ entonces $a \,/\, q$.

   Sea $p = ac$ y $p + q = ad$,

   entonces

$$q = ad - p$$

$$q = ad - ac$$

$$q = (d - c)a,$$

   de donde

$$a/q.$$

9. Si a/b, entonces a/mb, para todo $m \in \mathbb{Z}$.

   Sea $b = ac$,

   entonces

$$mb = mac = (mc)a.$$

   Por lo tanto

$$a/mb.$$

1.4 Máximo común divisor.

Definición 1.4.1

Sean a, b enteros con al menos uno de los dos diferente de cero. El máximo común divisor de a y b, denotado por $mcd(a,b)$, es el entero positivo d que satisface:

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

   c/a y c/b, entonces c/d.

Lema 1.4.2

Sean $a, b, q, r \in \mathbb{Z}$ tales que $a = bq + r$ con $b > 0$ y $0 \leq r < b$. Entonces $mcd(a,b) = mcd(b,r)$.

Demostración.

Sea $d = mcd(a,b)$,

entonces

d/a y $d \,/\, b$.

Por el numeral 7) del teorema 1.3.9 tenemos

$$d/(a - qb),$$

esto es

$$d/r.$$

De esta forma

$$d \,/\, mcd(b,r)$$

Así d es un divisor común de b y r.

Por otra parte si c es un divisor común arbitrario de b y r,

Por el numeral 7) del teorema 1.3.9 tenemos

$$c \,/\, (qb + r),$$

Y sabemos que

$$qb + r = a$$

De donde se tiene que

$$c \,/\, a.$$

Esto hace a c un divisor común de a y b, es decir que $c \leq d$. Así se sigue de la definición de $mcd(b, r)$ que $d = mcd(b, r)$. ■

Teorema 1.4.3

Dados dos enteros a y b, con al menos uno de los dos distintos de cero, el máximo común divisor entre a y b se expresa como combinación lineal de a y b. Es decir, existen enteros x e y tales que

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

Demostración.

Consideremos el conjunto S de todas las combinaciones lineales positivas de a y b.

$$S = \{au + bv / au + bv > 0 \,;\, u, v \; enteros\}$$

Notemos que S es no vacío. Si $a \neq 0$, entonces el entero $|a| = au + b \cdot 0$ está en S, donde elegimos $u = 1$ o $u = -1$ de acuerdo al valor de a. Por el principio del buen

orden S contiene un elemento mínimo d. Así de la definición de S existen enteros x e y para los cuales $d = ax + by$.

Del algoritmo de la división podemos obtener enteros q y r tales que

$$a = qd + r, \qquad 0 \leq r < d.$$

Reescribiendo r tenemos

$$r = a - qd = a - q(ax + by)$$
$$= a(1 - qx) + b(-qy).$$

Si $r > 0$, esta representación implica que r es un elemento de S, contradiciendo así que d es el menor entero en S.

Por lo tanto

$$r = 0 \quad \text{y} \quad a = qd,$$

es decir

$$d/a.$$

De igual forma del algoritmo de la división podemos obtener enteros q y r tales que

$$b = qd + r,\ 0 \leq r < d$$

Reescribiendo r tenemos

$$r = b - qd = b - q(ax + by)$$
$$= b(1 - qy) + a(-qx)$$

Si $r > 0$, esta representación implica que r es un elemento de S, contradiciendo así que d es el menor entero en S.

Por lo tanto

$$r = 0 \qquad \text{y} \qquad b = qd,$$

es decir

$$d/b.$$

Entonces vemos que d es un divisor común de a y b.

Sea un entero positivo arbitrario c un divisor común de los enteros a y b, entonces por el numeral 7) del teorema 1.3.9 sabemos que

$$c/ax + by \ ;$$

es decir que

$$c/d$$

Por el numeral 6) del teorema 1.3.9

$$\mathrm{c} = |c| \leq |d| = d,$$

de modo que d es el mas grande de todos los divisores comunes de a y b.

Así

$$d = mcd(a, b).$$

Definición 1.4.4

Dos enteros a y b, con al menos uno de ellos distinto de cero, son llamados primos relativos siempre que $mcd(a, b) = 1$.

Teorema 1.4.5

Sea a y b enteros, no ambos iguales a cero. Entonces a y b son primos relativos si y solo si existen enteros x e y tales que $1 = ax + by$.

Demostración.

"$\Longrightarrow$" Si a y b son primos relativos, entonces existen enteros x e y tales que

$$1 = ax + by.$$

Si a y b son primos relativos, entonces $mcd(a, b) = 1$.

Luego por el teorema 1.3.9 se garantiza la existencia de x e y los cuales satisfacen $1 = ax + by$.

"$\Longleftarrow$" Si existen enteros x e y tales que $1 = ax + by$, entonces a y b son primos relativos.

Supongamos que para algún x e y

$$1 = ax + by,$$

con $d = mcd(a, b)$.

Como d/a y d/b,

Por el numeral 7) del teorema 1.3.9 tenemos

$$d/ax + by,$$

es decir

$$d/1.$$

Como d es un entero positivo, la condición de divisibilidad $d/1$ obliga a que

$d = 1$. ■

Corolario 1.4.6

Si $mcd(a, b) = d$, entonces $mcd(a / d,\ b / d) = 1$.

Demostración.

Observemos que a/d y b/d aparentemente son fracciones, pero de hecho son enteros ya que d es un divisor común de a y de b.

Como sabemos que $mcd(a,b) = d$, es posible encontrar enteros x e y tales que $d = ax + by$. Dividiendo cada lado de esta ecuación por d, obtenemos la expresión

$$1 = (a/d)x + (b/d)y.$$

Como a/d y b/d son enteros, el teorema 1.4.5 se cumple. El resultado de esto es que a/d y b/d son primos relativos. ■

Corolario 1.4.7

Si a/c, b/c, y $mcd(a,b) = 1$, entonces ab/c.

Demostración.

Sea $c = ar$ y $c = bs$.

Como $mcd(a,b) = 1$, entonces para algunos x e y enteros se cumple

$$1 = ax + by.$$

Multiplicando esta igualdad por c tenemos

$$c = c(ax + by) = cax + cby.$$

Sustituyendo $c = ar$ y $c = bs$

$$c = (bs)ax + (ar)by$$

$$c = ab(sx + ry),$$

de donde se obtiene que ab/c. ■

Teorema 1.4.8 (Lema de Euclides)

Si a/bc, con $mcd(a,b) = 1$, entonces a/c.

Demostración.

Como $mcd(a,b) = 1$, del teorema 1.3.9 tenemos

$$1 = ax + by,$$

Donde x e y son enteros.

Multiplicando esta ecuación por c nos da

$$c = c(ax + by)$$

$$c = cax + cby.$$

Sabemos que a/a y por el numeral 9) del teorema 1.3.9 a/ac además, por hipótesis a/bc entonces por numeral 7) del teorema 1.3.9

$$a/(cax + cby),$$

para algunos enteros x e y.

Así sustituyendo $c = cax + cby$, tenemos

$$a/c. \quad \blacksquare$$

Definición 1.4.9

Sean a y b dos enteros positivos, el minimo común múltiplo entre a y b, es un entero positivo m, el cual satisface:

1. a/m y b/m.
2. Si e es otro entero, tal que a/e y b/e, se tiene m/e.

1.5 Números primos

Definición 1.5.1 (Primos y compuestos)

Un entero positivo p, distinto de 1, se dice que es un número primo, o simplemente primo, si los únicos divisores positivos de p son 1 y p. Si p no es primo, se dice que es compuesto.

El número 1 no se toma como primo solo por conveniencia. No perjudica en nada.

Se dice que a y b son primos relativos en el caso de que $mcd(a,b) = 1$ y que $b_1, b_2, \dots, b_n$ son primos relativos en el caso de que $mcd(b_1, b_2, \dots, b_n) = 1$.

Teorema 1.5.2

Si p es un número primo y p/ab, entonces p/a o p/b.

Demostración.

Si p/a no necesitamos probar nada más.

Asumimos que $p \nmid a$.

Como los únicos divisores de p son 1 y p, esto implica que $mcd(p,a) = 1$.

Del lema de Euclides tenemos que p/b. ■

Corolario 1.5.3

Si p es un número primo y $p/a_1 a_2 \dots a_n$, entonces p/a_k para algún k, donde $1 \leq k \leq n$.

Demostración.

La prueba la realizaremos por inducción sobre el número de factores n.

Si $n = 1$ se cumple ya que p/a .

Si $n = 2$ es una aplicación del teorema 1.5.2.

Supongamos que $n > 2$.

Sea

$$p/a_1a_2 \dots a_n$$

Por el teorema 1.5.2

$$p/a_n \qquad \text{o} \qquad p/a_1a_2 \dots a_{n-1}.$$

Si p/a_n se cumple y no hay nada más que probar. De otra forma en el caso de que $p/a_1a_2 \dots a_{n-1}$.

Por la hipótesis inductiva tenemos que

$$p/a_k$$

Para algún k, con $1 \leq k \leq n-1$.

En todo caso, p divide a uno de los enteros $a_1, a_2, \dots, a_n$. ■

Corolario 1.5.4

Si $p, q_1, q_2, \dots, q_n$ son todos primos y $p/q_1q_2 \dots q_s$, entonces $p = q_k$ para algún k, donde $1 \leq k \leq n$.

Prueba.

Del Corolario 1.5.3, sabemos que

$$p/q_k$$

Para algún $k,$ con $1 \leq k \leq n.$

Además sabemos que q_k es primo y por lo tanto sus únicos divisores positivos son 1 y el mismo q_k .

Como $p > 1,$ entonces no queda más que $p = q_k.$ ■

Teorema 1.5.5 (Teorema Fundamental de Aritmética)

Todo número entero positivo, mayor que uno, puede ser factorizado como un producto de números primos. Esta representación es única, apartando el orden en el cual aparecen los factores.

Demostración.

Sea n un número entero mayor que 1. Probaremos, primero, que n puede escribirse como un producto de números primos y, posteriormente, veremos que esa descomposición es, salvo en el orden de los factores, única.

Si n es primo, consideremos el número como producto de un solo factor y el teorema está demostrado.

Si n es compuesto, entonces existe un entero d tal que

$$d/n \quad \text{y} \qquad 1 < d < n\,.$$

Entre estos enteros d elegimos el más pequeño, llamémosle p_1, el cual debe ser un primo si no, es un número compuesto y tendría un divisor q con $1 < q < p_1$ entonces

$$q/p_1 \qquad \text{y} \qquad p_1/n$$

Implica que

$$q/n$$

Lo cual es una contradicción ya que hemos elegido a p_1 como el divisor más pequeño de n, distinto de 1.

Reescribiendo n tenemos

$$n = p_1 n_1$$

Donde p_1 es un primo y $1 < n_1 < n$.

Si n_1 es primo tenemos la factorización.

Si no, este proceso se repite para obtener otro número primo p_2 tal que $n_1 = p_2 n_2$ y así obtenemos $n = p_1 p_2 n_2$, con $1 < n_2 < n_1$.

Si n_2 es primo tenemos la factorización, de otra manera escribimos

$$n_2 = p_3 n_3,$$

donde n_3 es primo. Así tenemos

$$n = p_1 p_2 p_3 n_3, \qquad \text{con} \qquad 1 < n_3 < n_2.$$

Repitiendo este proceso un número finito de veces tenemos que n_{k-1} es un primo llamémosle p_k y así obtendremos

$n > n_1 > n_2 > \ldots > 1$.

Con lo cual llegamos a la factorización deseada

$n = p_1 p_2 \ldots p_k$.

Unicidad.

Supongamos que n puede descomponerse en factores primos de dos maneras distintas

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s \quad , \quad r \leq s$$

Donde los p_i y q_i son todos primos.

Reescribiendo los factores primos en orden creciente tenemos

$$p_1 \leq p_2 \leq \ldots p_r \, , q_1 \leq q_2 \leq \ldots \leq q_s$$

Como

$$n = p_1 p_2 \ldots p_k$$

Entonces

$$p_1 / n$$

De donde

$$p_1 / q_1 q_2 \ldots q_s$$

Del Corolario 1.5.4 tenemos que

$$p_1 = q_k, \qquad \text{para algún } k.$$

Pero

$$p_1 \geq q_1.$$

De esta misma forma obtenemos $q_1 \geq p_1$, de donde $p_1 = q_1$. Cancelando el factor común tenemos

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$$

Continuando con este proceso de cancelación, si $r < s$ llegamos a

$$1 = q_{r+1}q_{r+2} \ldots \ q_s$$

Lo cual es absurdo ya que cada q_i es primo y por ende $q_i > 1$.

Por lo tanto

$r = s \quad y \quad p_1 = q_1 , p_2 = q_2 , \ \ldots , p_r = q_r .$

Así las dos factorizaciones son iguales y esto completa la prueba. ■

Teorema 1.5.6

Existen infinitos números primos.

Demostración.

La prueba es por contradicción.

Los primeros números primos son 2, 3, 5,. . . Vemos que los números primos aparecen en orden ascendente.

Supongamos que hay un número finito de primos digamos

$$p_1, p_2, \ldots , p_n$$

Sea

$$P = p_1 p_2 \ldots \ p_n + 1$$

Entonces P es mayor que 1 y es distinto de todos los números primos de la lista.

Por el teorema fundamental de la aritmética P puede ser expresado como un producto de primos y por ende P es divisible por algún primo p. Pero

$$p_1, p_2 , \ldots , p_n$$

son los únicos números primos, de modo que p debe ser igual a alguno de los primos $p_1, p_2, \ldots, p_n$.

Sabemos que

$$p/p_1p_2 \ldots p_n$$

Y además

$$p/P$$

Por el numeral 7) del teorema 1.3.9 tenemos que

$$p/P - p_1p_2 \ldots p_n$$

Sustituyendo P tenemos

$$p/p_1p_2 \ldots p_n + 1 - p_1p_2 \ldots p_n$$

de donde

$$p/1 \quad (\leftrightarrow)$$

Lo cual es una contradicción ya que $p > 1$ y el único divisor de 1 es él mismo.

De donde hemos llegado a una contradicción y lo supuesto es falso y por lo tanto existen infinitos números primos. ■

Definición 1.5.7

Para cada entero positivo n, definimos $\phi(n)$ como el número de enteros positivos menores o iguales que n y primos relativos con n.

Definición 1.5.8

Un número de Fermat es un entero de la forma

$$F_n = 2^{2^n} + 1, \qquad n \geq 0.$$

Si F_n es primo, es llamado primo de Fermat.

CAPITULO II

TEORIA

DE

CONGRUENCIAS

2.1. Propiedades básicas de congruencias

Definición 2.1.1

Sea n un entero positivo, y a y b enteros.

Se dice que a es congruente a b, módulo n, en símbolos

$$a \equiv b \ (mod\ n)$$

Si n divide a $a - b$.

Es decir siempre y cuando $a - b = nk$, para algún $k \in \mathbb{Z}$.

En símbolos:

$$a \equiv b \ (mod\ n) \ \Leftrightarrow \ n \mid (a - b)$$

$$\Leftrightarrow \ a - b = nk, \ \ para\ algun\ k \in \mathbb{Z}.$$

Ejemplo 3:

Sea $n = 7$, tenemos que.

$3 \equiv 24 \ (mod\ 7)$ ya que $3 - 24 = -21 = (-3) \cdot 7$

$-31 \equiv 11 \ (mod\ 7)$ ya que $-31 - 11 = -42 = (-6) \cdot 7$

$-15 \equiv -64 \ (mod\ 7)$ ya que $-15 - (-64) = 49 = 7 \cdot 7$

Nota.

Cuando $n \nmid (a - b)$, entonces indicamos que a es incongruente a b módulo n y escribimos $a \not\equiv b \ (mod\ n)$.

Ejemplo 4:

$25 \not\equiv 12 \ (mod\ 7)$, la división por 7 falla en $25 - 12 = 13$.

Teorema 2.1.2

Cualesquiera dos enteros son congruentes módulo 1.

Demostración

$$a, b \in \mathbb{Z} \implies a - b \in \mathbb{Z}$$

$$\implies 1|(a-b)$$

$$\implies a \equiv b \ (mod\ 1) \quad \blacksquare$$

Teorema 2.1.3

Dos enteros son congruentes módulo 2 cuando son ambos pares o ambos impares.

Demostración

Sean $a, b \in \mathbb{Z}$

Caso 1. Cuando ambos son pares

$a = 2m$ y $b = 2n$, para $m, n \in \mathbb{Z}$

$$\implies b - a = 2n - 2m$$

$$= (n-m) \cdot 2$$

$$= r \cdot 2, \quad con\ r = n - m$$

$$\implies a \equiv b \ (mod\ 2).$$

Caso 2. Cuando ambos son impares

$a = 2m + 1$ y $b = 2n + 1$, para $m, n \in \mathbb{Z}$.

$$\implies b - a = 2n + 1 - (2m + 1)$$

$$= 2n + 1 - 2m - 1$$

$$= 2n - 2m$$

$$= (n - m) \cdot 2$$

$$= r \cdot 2, \quad con\, r = n - m$$

$\Longrightarrow a \equiv b\ (mod\ 2).$ ■

Nota.

En la práctica usual asumimos $n > 1$.

Dado un entero a, y sean q y r cociente y residuo sobre la división por n, además $a = qn + r, \quad 0 \leq r < n.$

Entonces por definición de congruencia

$a \equiv r\ (mod\ n)$ (Ya que $a - r = qn$).

Dado que hay n elecciones para r, vemos que todo entero es congruente módulo n en exactamente $0, 1, 2, 3, \ldots, n - 1$.

En particular $a \equiv 0\ (mod\ n)$ si y solo si $n|a$.

El conjunto de n enteros $0, 1, 2, 3, \ldots, n - 1$ es llamado “El menor conjunto de residuos positivos módulo n”.

En general.

Una colección de n enteros $a_1, a_2, \dots, a_n$ forman un conjunto completo de residuos (o un sistema completo de residuos) módulo n si todo entero es congruente módulo n para una y sólo una de las a_k.

Otra manera de escribirlo es que $a_1, a_2, \dots, a_n$ son congruentes módulo n para $0, 1, 2, 3, \dots, n-1$, tomando algún orden.

Ejemplo 5:

$-12, -4, 11, 15, 13, 22, 82, 91,$ constituyen un conjunto completo de residuos módulo 7.

Tenemos que

$-12 \equiv 2 \ (mod\ 7)$ $\quad$ $13 \equiv 6 \ (mod\ 7)$ $\quad$ $91 \equiv 0 \ (mod\ 7)$

$-4 \equiv 3 \ (mod\ 7)$ $\quad$ $22 \equiv 1 \ (mod\ 7)$

$11 \equiv 4 \ (mod\ 7)$ $\quad$ $82 \equiv 5 \ (mod\ 7)$

Teorema 2.1.4

Para enteros arbitrarios a y b, $a \equiv b \ (mod\ n)$ si y sólo si a y b admiten la división por n para algún residuo no negativo.

Demostración.

"$\Rightarrow$"

Por hipótesis

$$a \equiv b \ (mod\ n)$$

Es decir

$$a - b = kn, \ \ para\ algun\ k \in \mathbb{Z}$$

$$a = kn + b, \ \ para\ algun\ k \in \mathbb{Z}$$

Sobre la división por n en b quedan ciertos residuos r,

es decir

$b = qn + r, \quad 0 \leq r < n$ (1)

Luego,

$$\begin{aligned} a &= kn + b \\ &= kn + qn + r, && \text{por (1)} \\ &= (kn + qn) + r, && \text{asociatividad} \\ &= n(k + q) + r, && \text{factor común} \\ &= nt + r, && \text{con } t = k + q \end{aligned}$$

Significa que a tiene algún residuo como b.

$\therefore a$ y b admiten la división por n con residuo no negativo.

"⇐"

Supongamos que a y b admiten la división por n para algún residuo no negativo, es decir,

$a = q_1 n + r y b = q_2 n + r$, con algún residuo r $(0 \leq r < n)$

$$a - b = q_1 n + r - (q_2 n + r)$$

$$= q_1 n + r - q_2 n - r$$

$$= q_1 n - q_2 n$$

$$= n(q_1 - q_2)$$

$\Longrightarrow n|a-b$

$\Longrightarrow\ a \equiv b\ (mod\ n).$ ■

Ejemplo 6:

Dados los enteros -56 y -11 podemos expresarlos en la forma $-56 = (-7)\cdot 9 + 7$ y $-11 = (-2)\cdot 9 + 7$ con residuo 7.

Por Teorema 2.1.4, decimos que

$$-56 \equiv 11\ (mod\ 9).$$

En el otro sentido:

Si tenemos $-56 \equiv 11\ (mod\ 9)$

Entonces -56 y -11 tienen algún residuo común cuando se dividen por 9.

Teorema 2.1.5

Sea $n > 0$ un número fijo y a, b, c, d enteros arbitrarios.

Entonces se cumplen las siguientes propiedades:

(1) $a \equiv a\ (mod\ n).$ (Reflexiva)

(2) $a \equiv b\ (mod\ n) \Longrightarrow b \equiv a\ (mod\ n).$ (Simétrica)

(3) $a \equiv b\ (mod\ n)\ \wedge\ b \equiv c\ (mod\ n) \Longrightarrow a \equiv c\ (mod\ n).$ (Transitiva)

(4) $a \equiv b\ (mod\ n)\ \wedge\ c \equiv d\ (mod\ n) \Longrightarrow a + c \equiv b + d\ (mod\ n).$

(5) $a \equiv b\ (mod\ n)\ \wedge\ c \equiv d\ (mod\ n) \Longrightarrow ac \equiv bd\ (mod\ n).$

(6) $a \equiv b\ (mod\ n) \Longrightarrow a + c \equiv b + c\ (mod\ n)$.

(7) $a \equiv b\ (mod\ n) \Longrightarrow ac \equiv bc\ (mod\ n)$.

(8) $a \equiv b\ (mod\ n) \Longrightarrow a^k \equiv b^k (mod\ n)$, para cualquier entero positivo k.

Demostración.

(1) $a \equiv a\ (mod\ n)$

Para cualquier entero a tenemos

$$a - a = 0 \Longrightarrow a - a = 0 \cdot n$$

$$\Longrightarrow a \equiv a\ (mod\ n).$$

(2) $a \equiv b\ (mod\ n) \Longrightarrow b \equiv a\ (mod\ n)$

$$a \equiv b\ (mod\ n) \Longrightarrow a - b = kn,\ \ para\ algun\ k \in \mathbb{Z}$$

$$\Longrightarrow (-1) \cdot (a - b) = (-1) \cdot kn$$

$$\Longrightarrow -a + b = -kn$$

$$\Longrightarrow b - a = (-k) \cdot n$$

$$\Longrightarrow b \equiv a\ (mod\ n).$$

(3) $a \equiv b\ (mod\ n)\ \wedge\ b \equiv c\ (mod\ n) \Longrightarrow a \equiv c\ (mod\ n)$

Por hipótesis

$$a \equiv b\ (mod\ n)\ \wedge\ b \equiv c\ (mod\ n)$$

$$\Longrightarrow a - b = k_1 n\ \ \wedge\ \ b - c = k_2 n,\ \ para\ algunos\ k_1, k_2 \in \mathbb{Z}$$

$$\Longrightarrow a - b + (b - c) = k_1 n + k_2 n$$

$$\Longrightarrow a - b + b - c = (k_1 + k_2) n$$

$$\Longrightarrow a - c = kn\,, \quad donde \;\; k = k_1 + k_2$$

$$\Longrightarrow a \equiv c \;(mod\; n).$$

(4) $a \equiv b \;(mod\; n) \;\wedge\; c \equiv d \;(mod\; n) \Longrightarrow a + c \equiv b + d \;(mod\; n)$

Por hipótesis

$$a \equiv b \;(mod\; n) \;\wedge\; c \equiv d \;(mod\; n)$$

$$\Longrightarrow a - b = k_1 n \;\; \wedge \;\; c - d = k_2 n, \;\; para\; algunos\; k_1, k_2 \in \mathbb{Z}$$

$$\Longrightarrow (a - b) + (c - d) = k_1 n + k_2 n$$

$$\Longrightarrow a + (-b) + c + (-d) = (k_1 + k_2)n$$

$$\Longrightarrow a + [(-b) + c] + (-d) = kn\,, donde\; k = k_1 + k_2$$

$$\Longrightarrow a + [c + (-b)] + (-d) = kn$$

$$\Longrightarrow a + c + (-b) + (-d) = kn$$

$$\Longrightarrow (a + c) + [(-b) + (-d)] = kn$$

$$\Longrightarrow (a + c) + (-1)[b + d] = kn$$

$$\Longrightarrow (a + c) - (b + d) = kn$$

$$\Longrightarrow a + c \equiv b + d \;(mod\; n).$$

(5) $a \equiv b \;(mod\; n) \;\wedge\; c \equiv d \;(mod\; n) \Longrightarrow ac \equiv bd \;(mod\; n)$

Por hipótesis

$$a \equiv b \;(mod\; n) \;\wedge\; c \equiv d \;(mod\; n)$$

$$\Longrightarrow a - b = k_1 n \;\; \wedge \;\; c - d = k_2 n, \;\; para\; algunos\; k_1, k_2 \in \mathbb{Z}$$

$$\Longrightarrow a = b + k_1 n \;\; \wedge \;\; c = d + k_2 n$$

$$\Longrightarrow ac = (b + k_1 n)(d + k_2 n)$$

$$\Longrightarrow ac = bd + bk_2 n + dk_1 n + k_1 n k_2 n$$

$$\Longrightarrow ac = bd + (bk_2 + dk_1 + k_1k_2)n$$

$$\Longrightarrow ac = bd + kn\,,\ donde\ k = bk_2 + dk_1 + k_1k_2$$

$$\Longrightarrow ac - bd = kn$$

$$\Longrightarrow ac \equiv bd\ (mod\ n).$$

(6) $a \equiv b\ (mod\ n) \Longrightarrow a + c \equiv b + c\ (mod\ n)$

Por hipótesis

$a \equiv b\ (mod\ n)$.

Y por Propiedad (1)

$$c \equiv c\ (mod\ n)$$

$\Longrightarrow a + c \equiv b + c\ (mod\ n)$, Propiedad (4)

(7) $a \equiv b\ (mod\ n) \Longrightarrow ac \equiv bc\ (mod\ n)$

Por hipótesis

$$a \equiv b\ (mod\ n)$$

Y por Propiedad (1)

$$c \equiv c\ (mod\ n)$$

$\Longrightarrow ac \equiv bc\ (mod\ n)$, Propiedad (5)

(8) $a \equiv b\ (mod\ n) \Longrightarrow a^k \equiv b^k (mod\ n)$, para cualquier entero positivo k.

Por inducción

Para $k = 1$

$a \equiv b\ (mod\ n)$ se cumple.

Supongamos que se cumple para $k = n$.

Es decir

$$a^n \equiv b^n (mod\ n).$$

Probaremos que se cumple para $k = n + 1$.

Es decir

$$a^{n+1} \equiv b^{n+1} (mod\ n).$$

Tenemos por hipótesis inductiva que

$a^n \equiv b^n (mod\ n)$ y sabemos que $a \equiv b\ (mod\ n)$

$\Longrightarrow a^n \cdot a \equiv b^n \cdot b\ (mod\ n)$, Propiedad (5)

$\Longrightarrow a^{n+1} \equiv b^{n+1} (mod\ n).$

Se cumple para $k = n + 1$ y la prueba se completa. ■

Ejemplo 7:

Probar que $41 \mid 2^{20} - 1$

Solución.

Tenemos que $2^5 = 32 = 41 \cdot 1 - 9$

$\Longrightarrow 2^5 \equiv -9\ (mod\ 41)$

$\Longrightarrow (2^5)^4 \equiv (-9)^4 (mod\ 41)$, Propiedad (8)

$\Longrightarrow 2^{20} \equiv (-9)^2 \cdot (-9)^2 (mod\ 41)$

$\Longrightarrow 2^{20} \equiv 81 \cdot 81\ (mod\ 41)$

$$\Longrightarrow 2^{20} \equiv (-1)\cdot(-1)\ (mod\ 41), \quad \text{ya que } 81 \equiv -1\ (mod\ 41)$$

$$\Longrightarrow 2^{20} \equiv 1\ (mod\ 41)$$

$$\Longrightarrow 41 \mid 2^{20} - 1.$$

Teorema 2.1.6

Sea $n > 0$ un número fijo y a, b, c enteros arbitrarios.

Si tenemos que $ca \equiv cb\ (mod\ n)$, entonces $a \equiv b\ \left(mod\ \frac{n}{d}\right)$, donde

$d = mcd(c, n)$.

Demostración.

Por hipótesis tenemos que

$$ca \equiv cb\ (mod\ n) \Longrightarrow ca - cb = kn,\ \ para\ algun\ k \in \mathbb{Z}$$

$$\Longrightarrow c(a-b) = kn.$$

Ahora, como $d = mcd(c, n)$, entonces existen enteros primos relativos r, s tales que

$c = dr \ \wedge\ n = ds$.

Luego

$$c(a-b) = kn \Longrightarrow (dr)(a-b) = k(ds)$$

$$\Longrightarrow dr(a-b) = kds$$

$$\Longrightarrow dr(a-b) = dks$$

$$\Longrightarrow r(a-b) = ks$$

$$\Longrightarrow s \mid r(a-b)$$

$\Longrightarrow s \mid (a-b)$, ya que $mcd(r,s)=1$

$\Longrightarrow a-b=ts$, $para\ algún\ t \in \mathbb{Z}$

$\Longrightarrow a \equiv b\ (mod\ s)$

$\Longrightarrow a \equiv b\ (mod\ \frac{n}{d})$, ya que $s=\frac{n}{d}$ ■

Corolario 2.1.7

Sea $n>0$ un número fijo y a,b,c enteros arbitrarios.

Si tenemos que $ca \equiv cb\ (mod\ n)$ y $mcd(c,n)=1$, entonces $a \equiv b\ (mod\ n)$.

Demostración.

Por Teorema 2.1.5 tenemos que

$$ca \equiv cb\ (mod\ n) \Longrightarrow\ a \equiv b\ \left(mod\ \frac{n}{d}\right), \quad \text{donde } d=mcd(c,n).$$

Pero como $d=1$, entonces

$$a \equiv b\ \left(mod\ \frac{n}{1}\right) \Longrightarrow\ a \equiv b\ (mod\ n). \quad ■$$

2.2. Representación decimal de un número entero

Comenzaremos probando que dado un entero $b > 1$, cualquier entero positivo N puede ser escrito únicamente en términos de potencias de b como

$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$,

donde los coeficientes a_k en b pueden tomar diferentes valores

$a_k = 0, 1, 2, \ldots , b - 1.$

Por el algoritmo de la división, se pueden producir enteros q_1 y a_0 que satisfacen que

$$N = q_1 b + a_0 \qquad 0 \leq a_0 < b \qquad (1)$$

Si

$$q_1 > b$$

Podemos dividir una vez más y tenemos

$$q_1 = q_2 b + a_1 \qquad 0 \leq a_1 < b$$

Luego sustituyendo q_1 en (1) tenemos

$$N = (q_2 b + a_1) b + a_0$$

$$\Longrightarrow N = q_2 b^2 + a_1 b + a_0 , \qquad siempre\ que\ q_2 > b. \qquad (2)$$

Podemos continuar de la misma manera

$$q_2 = q_3 b + a_2 \qquad 0 \leq a_2 < b$$

Luego sustituyendo en (2)

$$N = q_2 b^2 + a_1 b + a_0$$

$$\Longrightarrow N = (q_3 b + a_2) b^2 + a_1 b + a_0$$

$$\Longrightarrow N = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

Donde

$$N > q_1 > q_2 > \cdots > 0$$

Es una sucesión de enteros estrictamente decrecientes.

Este proceso termina cuando se llega a $m - 1$ etapas, donde

$q_{m-1} = q_m b + a_{m-1}$, $\quad 0 \leq a_{m-1} < b \;\; y \;\; 0 \leq q_m < b.$

Sustituyendo a_m por q_m llegamos a la representación de N

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

Para probar que N tiene representación única lo hacemos por contradicción suponiendo que N tiene dos representaciones.

Sean

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0 \,, \quad con\ 0 \leq a_i < b, \forall i \qquad (1)$$

Y $\quad N = c_m b^m + c_{m-1} b^{m-1} + \cdots + c_2 b^2 + c_1 b + c_0 \,, \quad con\ 0 \leq c_j < b, \forall j \qquad (2)$

Tales representaciones.

Restando (2) de (1) tenemos

$$N - N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0 - (c_m b^m + c_{m-1} b^{m-1} + \cdots + c_2 b^2 + c_1 b + c_0)$$

$$\Rightarrow 0 = a_m b^m + a_{m-1}b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0 - c_m b^m - c_{m-1}b^{m-1} - \cdots - c_2 b^2 - c_1 b - c_0$$

$$\Rightarrow 0 = (a_m b^m - c_m b^m) + (a_{m-1}b^{m-1} - c_{m-1}b^{m-1}) + \cdots + (a_2 b^2 - c_2 b^2) + (a_1 b - c_1 b) + (a_0 - c_0)$$

$$\Rightarrow 0 = (a_m - c_m)b^m + (a_{m-1} - c_{m-1})b^{m-1} + \cdots + (a_2 - c_2)b^2 + (a_1 - c_1)b + (a_0 - c_0)$$

$$\Rightarrow 0 = d_m b^m + d_{m-1}b^{m-1} + \cdots + d_2 b^2 + d_1 b + d_0 \ , \qquad \text{con } d_i = a_i - c_i \ , \forall i.$$

Ya que hemos supuesto que (1) y (2) son distintas tenemos que $d_i \neq 0$, para algunos valores de i.

Tomemos un k, el más pequeño para el cual $d_k \neq 0$, entonces

$$0 = d_m b^m + d_{m-1}b^{m-1} + \cdots + d_{k+1}b^{k+1} + d_k b^k$$

$$\Longrightarrow -d_k b^k = d_m b^m + d_{m-1}b^{m-1} + \cdots + d_{k+1}b^{k+1}$$

$$\Longrightarrow (-1)(-d_k b^k) = (-1)(d_m b^m + d_{m-1}b^{m-1} + \cdots + d_{k+1}b^{k+1})$$

$$\Longrightarrow d_k b^k = -d_m b^m - d_{m-1}b^{m-1} - \cdots - d_{k+1}b^{k+1}$$

Y al dividir por b^k tenemos que

$$d_k = -d_m b^{m-k} - d_{m-1}b^{m-k-1} - \cdots - d_{k+1}b^{k-k+1}$$

$$\Longrightarrow d_k = -d_m b^{m-k} - d_{m-1} b^{m-k-1} - \cdots - d_{k+1} b$$

$$\Longrightarrow d_k = b(-d_m b^{m-k-1} - d_{m-1} b^{m-k-2} - \cdots - d_{k+1})$$

$$\Longrightarrow d_k = bs\,, \quad con\ s = -d_m b^{m-k-1} - d_{m-1} b^{m-k-2} - \cdots - d_{k+1}$$

$$\Longrightarrow b \mid d_k$$

Tenemos las desigualdades

$$0 < a_k < b \quad \text{y} \quad 0 < c_n < b$$

$$0 < c_n < b \Longrightarrow 0 > -c_n > -b$$

$$\Longrightarrow -b < -c_n < 0$$

$$\Longrightarrow 0 - b < a_k - c_k < b + 0$$

$$\Longrightarrow -b < a_k - c_k < b$$

$$\Longrightarrow -b < d_k < b$$

$$\Longrightarrow | d_k | < b$$

Entonces tenemos que $b \mid d_k$ y $| d_k | < b$ lo cual implica que $d_k = 0$ $(\longrightarrow\longleftarrow)$

Por lo tanto N tiene representación única. ■

Nota.

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

Puede ser reemplazado por el símbolo

$$N\colon (\, a_m a_{m-1} \cdots a_2 a_1 a_0)_b$$

Ejemplo 8

El número 105 puede ser escrito en potencia de base $b = 2$.

Solución.

Tenemos que

$$105 = 2 \cdot (52) + 1$$

$$\Longrightarrow 105 = 2 \cdot (2 \cdot (26) + 0) + 1$$

$$\Longrightarrow 105 = 2^2 \cdot (26) + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^2 \cdot (2 \cdot (13) + 0) + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^3 \cdot (13) + 2^2 \cdot 0 + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^3 \cdot (2 \cdot 6 + 1) + 2^2 \cdot 0 + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^4 \cdot 6 + 2^3 \cdot 1 + 2^2 \cdot 0 + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^4 \cdot (2 \cdot 3 + 0) + 2^3 \cdot 1 + 2^2 \cdot 0 + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^5 \cdot 3 + 2^4 \cdot 0 + 2^3 \cdot 1 + 2^2 \cdot 0 + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^5 \cdot (2 \cdot 1 + 1) + 2^4 \cdot 0 + 2^3 \cdot 1 + 2^2 \cdot 0 + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 2^6 \cdot 1 + 2^5 \cdot 1 + 2^4 \cdot 0 + 2^3 \cdot 1 + 2^2 \cdot 0 + 2 \cdot 0 + 1$$

$$\Longrightarrow 105 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1$$

$$\Longrightarrow 105 = 2^6 + 2^5 + 2^3 + 1.$$

En forma abreviada

$105 = (\,1101001)_2$.

Teorema 2.2.1

Sea $P(x) = \sum_{k=0}^{m} c_k x^k$ una función polinomial de x con coeficientes enteros c_k.

Si $a \equiv b \ (mod\ n)$, entonces $P(a) \equiv P(b) \ (mod\ n)$.

Demostración.

Por hipótesis $a \equiv b \ (mod\ n)$

$$a \equiv b \ (mod\ n) \Longrightarrow a^k \equiv b^k (mod\ n), \ \ \forall k \in \mathbb{Z} \quad \{Teo.\ 2.1.2\ Propiedad\ (8)\}$$

$$\Longrightarrow c_k a^k \equiv c_k b^k (mod\ n), \ \ \forall k \in \mathbb{Z} \quad \{Teo.\ 2.1.2\ Propiedad\ (7)\}$$

Como esto se cumple entonces tenemos que

$c_0 \equiv c_0 (mod\ n),\ c_1 a \equiv c_1 b \ (mod\ n), \ldots,\ c_m a^m \equiv c_m b^m (mod\ n).$

Entonces por Teorema 2.1.5 Propiedad (4)

$$(c_0 + c_1 a + c_2 a^2 + \cdots + c_m a^m) \equiv (c_0 + c_1 b + c_2 b^2 + \cdots + c_m b^m) \ (mod\ n)$$

$$\Longrightarrow \sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \ \ (mod\ n)$$

$\Longrightarrow P(a) \equiv P(b) \ (mod\ n).$ ■

Corolario 2.2,2

Si a es una solución de $P(x) \equiv 0 \ (mod\ n)$ y $a \equiv b \ (mod\ n)$, entonces b es también una solución.

Demostración.

Si a es una solución de $P(x) \equiv 0\ (mod\ n)$, entonces $P(a) \equiv 0\ (mod\ n)$.

Ahora por Teorema 2.2.1 tenemos que

Si

$$a \equiv b\ (mod\ n)$$

Entonces

$$P(a) \equiv P(b)\ (mod\ n)$$

Y por Teorema 2.1.5 Propiedad (2) y (3) tenemos que

$$0 \equiv P(a) \equiv P(b)(mod\ n) \Longrightarrow P(b) \equiv 0\ (mod\ n)$$

Por tanto b también es una solución de $P(x) \equiv 0\ (mod\ n)$. ■

Teorema 2.2.3

Sea $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ la representación decimal de un entero positivo N, $0 \leq a_k < 10$, y sea $S = a_0 + a_1 + a_2 + \cdots + a_m$. Entonces $9 \mid N$ si y sólo si $9 \mid S$.

Demostración.

Sea $P(x) = \sum_{k=0}^{m} a_k x^k$ un polinomio con coeficientes enteros a_k.

Sabemos por Teorema 2.2.1 que

Si

$$10 \equiv 1\ (mod\ 9)$$

Entonces

$$P(10) \equiv P(1)\ (mod\ 9)$$

Luego,

$$P(10) = \sum_{k=0}^{m} a_k 10^k$$

$$= a_0 + a_1 10 + a_2 10^2 + \cdots + a_{m-1} 10^{m-1} + a_m 10^m$$

$$= N$$

$$P(1) = \sum_{k=0}^{m} a_k 1^k$$

$$= a_0 + a_1 + a_2 + \cdots + a_{m-1} + a_m$$

$$= S.$$

Entonces

$$P(10) \equiv P(1)\ (mod\ 9) \Longrightarrow N \equiv S\ (mod\ 9)$$

Y por el Corolario 2.2.2

$$N \equiv 0\ (mod\ 9) \Leftrightarrow S \equiv 0\ (mod\ 9)$$

$$\Longrightarrow \quad 9 \mid N \Leftrightarrow 9 \mid S. \qquad \blacksquare$$

Teorema 2.2.4

Sea $N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$ la representación decimal de un entero positivo N, $0 \leq a_k < 10$, y sea $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Entonces $11 \mid N$ si y sólo si $11 \mid T$.

Demostración.

Sea $P(x) = \sum_{k=0}^{m} a_k x^k$ un polinomio con coeficientes enteros a_k.

Por Teorema 2.2.1

Si

$$10 \equiv -1 \ (mod\ 11)$$

Entonces

$$P(11) \equiv P(-1)(mod\ 11).$$

Luego,

$$P(10) = \sum_{k=0}^{m} a_k 10^k$$

$$= a_0 + a_1 10 + a_2 10^2 + \cdots + a_{m-1} 10^{m-1} + a_m 10^m$$

$$= N.$$

$$P(-1) = \sum_{k=0}^{m} a_k 1^k$$

$$= a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$$

$$= T.$$

Entonces

$$P(11) \equiv P(-1) \ (mod\ 11) \Longrightarrow N \equiv T \ (mod\ 11).$$

Y por el Corolario 2.2.2

$$N \equiv 0 \ (mod\ 11) \Leftrightarrow S \equiv 0 \ (mod\ 11)$$

$$\Longrightarrow \quad 11 \mid N \Leftrightarrow 11 \mid S. \qquad \blacksquare$$

2.3. Congruencias lineales

En Algebra se estudian detalladamente las ecuaciones polinómicas y sus soluciones. En forma análoga podemos estudiar las congruencias polinómicas.
En este trabajo consideramos únicamente polinomios $P(x)$ con coeficientes enteros.

Si a es un entero tal que $P(a) \equiv 0\ (mod\ n)$, decimos que a es una solución de la congruencia polinómica $P(x) \equiv 0\ (mod\ n)$. Por el Teorema 2.2.1, Si $a \equiv b\ (mod\ n)$ también $P(a) \equiv P(b)\ (mod\ n)$, sin embargo no consideramos diferentes a estas soluciones que pertenecen a una misma clase de residuos módulo n. Cuando hablamos del número de soluciones de una congruencia polinómica nos referimos al número de soluciones incongruentes, es decir al número de soluciones obtenidas en el conjunto $\{0, 1, 2, \dots, n-1\}$ o en cualquier otro sistema completo de residuos módulo n.

La congruencia $P(x) \equiv 0\ (mod\ n)$ se llama lineal cuando $P(x)$ es un polinomio de grado uno. Toda congruencia lineal se puede escribir en la forma
$ax \equiv b\ (mod\ n)$.
Tenemos el resultado siguiente.

Teorema 2.3.1

La congruencia lineal $ax \equiv b\ (mod\ n)$ tiene una solución si y sólo si $d|b$, donde $d = mcd(a, n)$.

Si $d|b$, entonces tiene d soluciones incongruentes modulo n.

Demostración.

$$ax \equiv b\ (mod\ n) \Leftrightarrow ax - b = ny\ ,\quad para\ algun\ y \in \mathbb{Z}$$

$$\Leftrightarrow ax - ny = b$$

$$\Leftrightarrow d|b.$$

Sea x_0, y_0 una solución particular. Si x', y' es otra solución entonces

$$ax_0 - ny_0 = b \qquad \text{y} \qquad ax' - ny' = b.$$

De donde

$$ax_0 - ny_0 = ax' - ny'$$

$$\Longrightarrow ny' - ny_0 = ax' - ax_0$$

$$\Longrightarrow n(y' - y_0) = a(x' - x_0) \qquad (1)$$

Por el definición 1.3.8, existen enteros primos relativos r y s tales que

$$a = dr, \qquad n = ds.$$

$$\Longrightarrow\ a/d = r, \qquad n/d = s.$$

Sustituyendo estos valores en (1) tenemos

$$ds(y' - y_0) = dr(x' - x_0)$$

$$\Longrightarrow s(y' - y_0) = r(x' - x_0).$$

Luego

$$s|r(x' - x_0),\quad con\ \ mcd(s, r) = 1.$$

Usando el lema de Euclides tenemos que

$$s|(x' - x_0)$$

$$\Longrightarrow x' - x_0 = st, \quad para\ algun\ \ t \in \mathbb{Z}$$

$$\Longrightarrow x' - x_0 = \frac{n}{d}t$$

$$\Longrightarrow x' = x_0 + \frac{n}{d}t.$$

Sustituyendo $x' - x_0 = st$ obtenemos

$$s(y' - y_0) = r(x' - x_0)$$

$$\Longrightarrow s(y' - y_0) = rst$$

$$\Longrightarrow y' - y_0 = rt$$

$$\Longrightarrow y' - y_0 = \frac{a}{d}t$$

$$\Longrightarrow y' = y_0 + \frac{a}{d}t \quad .$$

Entonces cualquier otra solución tiene la forma

$$x = x_0 + \frac{n}{d}t\ ,\ y = y_0 + \frac{a}{d}t,$$

para algunos $t \in \mathbb{Z}$.

Consideremos que estas soluciones ocurren cuando t toma valores sucesivos $t = 0, 1, 2, \dots, d - 1$.

Entonces afirmamos que los enteros

$$x_0, \qquad x_0 + \frac{n}{d}t, \qquad x_0 + \frac{2n}{d}t, \dots , \qquad x_0 + \frac{(d-1)n}{d}t$$

son incongruentes módulo n, todos los demás enteros tales que x es congruente con alguno de ellos

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \ (mod\ n).$$

Donde $0 \leq t_1 \leq t_2 \leq d - 1$.

$$\Longrightarrow \quad \frac{n}{d}t_1 \ \equiv \ \frac{n}{d}t_2 \ (mod\ n).$$

Luego

$$mcd\left(\frac{n}{d}, n\right) = \frac{n}{d}.$$

$$\Longrightarrow t_1 \equiv t_2 \ (mod\ n),$$

$$\Longrightarrow d \mid t_1 - t_2$$

$$\Longrightarrow d \mid t_2 - t_1 \quad (\leftrightarrow)$$

Es una contradicción ya que $0 < t_2 - t_1 < d$.

Por el algoritmo de la división

$$t = qd + r \quad , \quad 0 \leq r < d - 1$$

$$x_0 + \frac{n}{d}t \equiv x_0 + \frac{n}{d}t \ (mod\ n)$$

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r)$$

$$= x_0 + nq + \frac{nr}{d}$$

$$\Longrightarrow x_0 + \frac{n}{d}t \; - \; \frac{nr}{d} = x_0 + nq$$

$$\Longrightarrow x_0 + \frac{n}{d}t \; - x_0 - \frac{nr}{d} = nq$$

$$\Longrightarrow \left(x_0 + \frac{n}{d}t\right) - \left(x_0 + \frac{nr}{d}\right) = nq$$

$$\Longrightarrow x_0 + \frac{n}{d}t \; \equiv \; x_0 + \frac{n}{d}r \; (mod\; n).$$

Con $x_0 + (n/d)r$.

Esto completa la prueba. ■

Ejemplo 9:

Resolvamos la congruencia lineal $32x \equiv 28\ (mod\ 36)$.

Solución.

Como

$$mcd(32{,}36) = 4 \quad \text{y} \quad 4 \mid 28,$$

La congruencia tiene 4 soluciones incongruentes.

Utilizando propiedades de las congruencias, la congruencia dada es equivalente a cada una de las congruencias siguientes.

$$32x \equiv 28\ (mod\ 36)$$

$$8x \equiv 7\ (mod\ 9) \quad , \quad \text{Teo. 2.1.5}$$

$$-x \equiv 7\ (mod\ 9)$$

$$x \equiv -7 \ (mod\ 9)$$

$$x \equiv 2 \ (mod\ 9).$$

Por el teorema sabemos que las soluciones incongruentes están dadas por

$x_0 + (n/d)r$. Con $r = 0, 1, 2, 3$.

Por lo tanto las soluciones incongruentes son 2, 11, 20 y 29.

Teorema 2.3.2

Consideremos la congruencia lineal $ax \equiv b \ (mod\ n)$. Si y_0 es una solución de la congruencia $ny \equiv -b \ (mod\ a)$, entonces el número

$$x_0 = \frac{ny_0 + b}{a}$$

Es una solución de la congruencia original.

Demostración.

Como y_0 es solución de la congruencia $ny \equiv -b \ (mod\ a)$, entonces x_0 es un entero y además

$$ax_0 = a\frac{ny_0 + b}{a}$$

$$\Longrightarrow ax_0 = ny_0 + b$$

$$\Longrightarrow ax_0 - b = ny_0$$

$$\Longrightarrow ax_0 \equiv b \ (mod\ n).$$

Luego x_0 es solución de $ax \equiv b\ (mod\ n)$. ■

Ejemplo 10

Resolvamos la congruencia $245 \equiv 64\ (mod\ 9923)$, usando el teorema anterior.

Solución.

Por el teorema 2.3.2 nos reducimos a resolver la congruencia

$$9923y \equiv -64\ (mod\ 245).$$

O sea

$$123y \equiv -64\ (mod\ 245).$$

Nuevamente por el teorema 2.3.2, nos reducimos a resolver la siguiente congruencia

$$245z \equiv -(-64)(mod\ 123),$$

o sea

$$122z \equiv 64\ (mod\ 123)$$

$$\Longrightarrow \quad -z \equiv 64\ (mod\ 123)$$

$$\Longrightarrow \quad (-1)(-z) \equiv (-1)(64)\ (mod\ 123)$$

$$\Longrightarrow \quad z \equiv -64\ (mod\ 123)$$

$$\Longrightarrow \quad z \equiv 59\ (mod\ 123).$$

Luego

$$y_0 = \frac{(245)(59) - 64}{123} = 117$$

Y $x_0 = \frac{(9923)(117)+64}{245} = 4739.$

Nota.

Cuando apliquemos el teorema anterior a una congruencia $ax \equiv b\ (mod\ n)$ donde $mcd(a,n) \nmid b$, es claro que el proceso nos conducirá a una congruencia que no tiene solución.

Teorema 2.3.3 (Teorema Chino del Residuo)

Sean $m_1, m_2, \ldots, m_r$ enteros positivos primos relativos dos a dos, y sean $a_1, a_2, \ldots, a_r$ enteros arbitrarios. Entonces el sistema de congruencias lineales

$$x \equiv a_1 (mod\ m_1)$$

$$x \equiv a_2 (mod\ m_2)$$

$$\vdots$$

$$x \equiv a_r (mod\ m_r)$$

Tiene solución única módulo $m = \prod_{i=1}^{r} m_i$.

Demostración.

Para

$$i = 1, 2, \ldots, r$$

Sea

$$M_i = \frac{m}{m_i} = \prod_{i \neq j} m_j$$

Entonces

$$mcd(M_i, m_i) = 1 \text{ para todo } i.$$

Por el Teorema 2.3.2 existen soluciones únicas para las congruencias lineales

$M_i x \equiv 1 \ (mod\ m_i)$, para $i = 1, 2, \dots, r$.

Es decir existen enteros $b_1, b_2, \dots, b_r$ tales que

$M_1 b_1 \equiv 1 \ (mod\ m_1),\ M_2 b_2 \equiv 1 \ (mod\ m_2), \dots\ ,\ M_r b_r \equiv 1 \ (mod\ m_r)$.

Por lo tanto,

$M_1 b_1 a_1 \equiv a_1 (mod\ m_1),\ M_2 b_2 a_2 \equiv a_2 (mod\ m_2), \dots\ ,\ M_r b_r a_r \equiv a_r \ (mod\ m_r)$.

Y si establecemos

$$x_0 = \sum_{i=1}^{r} M_i b_i a_i.$$

Tenemos que

$$x_0 \equiv a_i \ (mod\ m_i) \text{ para todo } i$$

Puesto que

$$M_i \equiv 0 \ (mod\ m_j) \text{ para } i \neq j.$$

En consecuencia, x_0 es una solución del sistema de congruencias.

Supongamos ahora que x_1 y x_0 son dos soluciones del sistema.

Entonces

$$x_1 \equiv a_i \equiv x_0 \ (mod\ m_i)$$

Para $i = 1, 2, \dots, r$.

Y concluimos que

$$x_1 \equiv x_0 \ (mod\ m) \text{ donde } m = \prod_{i=1}^{r} m_i.$$

Por consiguiente, la solución es única módulo m. ■

2.4. Teoremas importantes

Teorema 2.4.1 (Teorema de Fermat).

Si p es un número primo y $(a, p) = 1$, entonces $a^{p-1} \equiv 1 \ (mod\ p)$.

Demostración.

Sea

$$\{r_1, r_2, \dots, r_{p-1}\},$$

un sistema reducido de residuos módulo n.

Sabemos que el conjunto $\{ar_1, ar_2, \dots, ar_{p-1}\}$ es también un sistema reducido de residuos módulo n.

Por lo tanto el producto de los enteros del primer conjunto es congruente al producto de los enteros del segundo conjunto. Luego

$$r_1 r_2 \cdots r_{p-1} \equiv a^{p-1} r_1 r_2 \cdots r_{p-1} (mod\ n).$$

Como cada r_i es primo relativo con n, podemos cancelar cada uno de los r_i y obtenemos

$$1 \equiv a^{p-1} \ (mod\ p)$$

Como queríamos probar. ■

Teorema 2.4.2 (Teorema de Wilson).

Para todo número primo p se tiene que

$$(p-1)! + 1 \equiv 0 \ (mod\ p)$$

Demostración.

Consideremos el polinomio de grado $p-2$ definido por

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - (x^{p-1} - 1)$$

Por el Teorema de Fermat, cada uno de los números $1, 2, \ldots, p-1$ es una solución de la congruencia $f(x) \equiv 0(mod\ p)$.

Tenemos que los coeficientes de $f(x)$ son divisibles por p, en particular el término constante

$$f(0) = (-1)^{p-1}(p-1)! + 1$$

Es divisible por p, o sea

$$(-1)^{p-1}(p-1)! + 1 \equiv 0 \ (mod\ p)$$

Si p es impar

$$(-1)^{p-1} = 1$$

y si $p = 2$

$$(-1)^{p-1} = -1 \equiv 1 \ (mod\ p).$$

Luego en cualquier caso

$$(p-1)! + 1 \equiv 0 \ (mod\ p). \quad \blacksquare$$

Teorema 2.4.3 (Teorema de Lagrange).

Si p es un número primo y $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ es un polinomio de grado $n \geq 1$ con coeficientes enteros y tal que $a_n \not\equiv 0 \ (mod\ p)$, entonces la congruencia polinómica

$$f(x) \equiv 0 \ (mod\ p)$$

tiene a lo sumo n soluciones incongruentes módulo p.

Demostración

La demostración es por inducción sobre el grado n de $f(x)$.

Cuando $n = 1$, la congruencia es lineal,

$a_0 + a_1 x \equiv 0 \ (mod\ p)$,

con $a_1 \not\equiv 0 \ (mod\ p)$ y por el Teorema 2.3.1, esta congruencia tiene exactamente una solución.

Supongamos que el teorema es cierto para polinomios de grado $n - 1$.

Consideremos un polinomio $f(x)$ de grado n y escojamos una solución a la congruencia $f(x) \equiv 0\ (mod\ p)$. Podemos escribir

$f(x) = (x-a)g(x) + r,$

con r constante y $g(x)$ un polinomio de grado $n-1$ con coeficientes enteros y coeficiente principal a_n.

De la ecuación anterior tenemos $f(a) = r$ y como $f(a) \equiv 0\ (mod\ p)$, entonces $r \equiv 0\ (mod\ p)$ y para todo x tenemos que

$$f(x) \equiv (x-a)g(x)\ (mod\ p). \qquad (*)$$

Por la hipótesis de inducción la congruencia $g(x) \equiv 0\ (mod\ p)$ tiene a lo más $n-1$ soluciones incongruentes. Supongamos que ellas son $c_1, \dots, c_r$ con $r \leq n-1$. Si c es un número tal que $f(c) \equiv 0\ (mod\ p)$, entonces de (*)

$$(c-a)g(c) \equiv 0\ (mod\ p)$$

así que

$$c \equiv a\ (mod\ p)$$

o

$$g(c) \equiv 0\ (mod\ p)$$

En el último caso $c = c_i$ para algún i con $1 \leq i \leq r$ y la congruencia

$f(x) \equiv 0\ (mod\ p)$ tiene a lo más $r+1 \leq n$ soluciones.

Luego el teorema es verdadero. ■

También tenemos que enunciar unas definiciones importantes y necesarias.

Definición 2.4.4

Sea n un entero positivo y a un entero tal que $(a, n) = 1$.

El menor entero positivo k tal que $a^k \equiv 1\ (mod\ n)$ se llama orden de a módulo n y lo representamos por la notación $ord_n\ a$.

Definición 2.4.5

Si $ord_n\ a = \phi(n)$, decimos que a es una raíz primitiva módulo n.

CAPITULO

III

LA LEY DE RECIPROCIDAD CUADRATICA

3.1. Congruencias de segundo grado con módulo primo y el Criterio de Euler.

Una congruencia cuadrática con módulo primo p tiene la forma,

$$ax^2 + bx + c \equiv 0 \ (mod\ p) \qquad (1)$$

Donde p es un primo impar y $a \not\equiv 0 \ (mod\ p)$, es decir, $mcd(a, p) = 1$.

La suposición que p es un primo impar implica que $mcd(4a, p) = 1$. Así, la congruencia cuadrática (1) es equivalente a

$$4a(ax^2 + bx + c) \equiv 0 \ (mod\ p)$$

Usando la identidad

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$$

La última congruencia cuadrática escrita puede ser expresada como

$$(2ax + b)^2 \equiv (b^2 - 4ac)(mod\ p)$$

Ahora, hacemos $y = 2ax + b$ y $d = b^2 - 4ac$ para obtener

$$y^2 \equiv d \ (mod\ p) \qquad (2)$$

Si $x \equiv x_0 (mod\ p)$ es una solución de la congruencia cuadrática (1), entonces el entero $y \equiv 2ax_0 + b (mod\ p)$ satisface la congruencia cuadrática (2).

De manera inversa tenemos que si $y \equiv y_0 (mod\ p)$ es una solución de la congruencia cuadrática (2), entonces $2ax \equiv y_0 - b\ (mod\ p)$ puede ser resuelto para obtener una solución de (1).

Así, el problema de encontrar una solución a la congruencia cuadrática (1) es equivalente a encontrar una solución a la congruencia lineal y una solución a la congruencia cuadrática de la forma

$$x^2 \equiv a\ (mod\ p) \qquad (3)$$

Si $p|a$, entonces la congruencia cuadrática (3) tiene a $x \equiv 0\ (mod\ p)$ como única solución. Para evitar trivialidades, acordaremos asumir de ahora en adelante que $p \nmid a$.

De acuerdo con lo anterior, siempre que $x^2 \equiv a\ (mod\ p)$ admite una solución $x = x_0$, entonces existe también una segunda solución $x = p - x_0$. Esta segunda solución es no congruente a la primera.

Para

$$x_0 \equiv p - x_0\ (mod\ p)$$

Implica que

$$2x_0 \equiv 0\ (mod\ p) \qquad \text{o} \qquad x_0 \equiv 0\ (mod\ p)$$

Lo cual es imposible.

Por Teorema de Lagrange, esas dos soluciones agotan las soluciones incongruentes de $x^2 \equiv a(mod\ p)$.

Por tanto: $x^2 \equiv a\ (mod\ p)$ tiene exactamente dos soluciones o no tiene soluciones.

Ejemplo 11:

Un ejemplo numérico de lo que acabamos de decir proporcionado por la congruencia cuadrática

$$5x^2 - 6x + 2 \equiv 0\ (mod\ 13)$$

Para obtener la solución, uno reemplaza esta congruencia por una más sencilla.

De la ecuación tenemos que

$$a = 5,\ \ b = -6 \text{ y } c = 2$$

Entonces

$$d = b^2 - 4ac$$

$$d = (-6)^2 - 4(5)(2) = -4$$

Además

$$-4 \equiv 9\ (mod\ 13)$$

Así obtenemos la congruencia

$$y^2 \equiv 9\ (mod\ 13)$$

Con soluciones

$$y \equiv 3, 10\ (mod\ 13).$$

Después, resolver las congruencias lineales

$$10x \equiv 9\ (mod\ 13),\ 10x \equiv 16\ (mod\ 13)$$

No es difícil ver que $x \equiv 10, 12 \ (mod\ 13)$ satisfacen esas ecuaciones y, por nuestra observación previa, también la congruencia cuadrática original.

El esfuerzo mayor en esta presentación es directa para obtener una prueba para la existencia de soluciones de la congruencia cuadrática

$$x^2 \equiv a \ (mod\ p),\ mcd(a,p) = 1. \qquad (4)$$

Dicho de otro modo, deseamos identificar que estos enteros son cuadrados perfectos módulo p.

Algunos términos adicionales ayudaran a discutir esta situación de una manera concisa.

Para cualquier modulo, todos los números pueden separarse en dos clases, una de las cuales contiene los números que pueden ser congruentes a algún cuadrado, la otra contiene los que no pueden serlo. Cada clase de éstos se define de la siguiente manera:

Definición 3.1.1

Sea p un primo impar y a un entero con $mcd(a,p) = 1$. Si la congruencia $x^2 \equiv a \ (mod\ p)$ tiene una solución, a se dice que es un residuo cuadrático de p, de otro modo, a es llamado un residuo no cuadrático de p.

Lo que se debe tener siempre en cuenta es que si $a \equiv b \ (mod\ p)$, entonces a es un residuo cuadrático de p si y solo si b es un residuo cuadrático de p.

Así, necesitamos determinar solo el carácter cuadrático de estos enteros positivos menores que p en orden, para analizar cualquier entero.

Ejemplo 12:

Consideremos el caso del primo $p = 13$.

Para encontrar cuantos de los enteros $1, 2, 3, \dots, 12$ son residuos cuadráticos de 13, debemos saber cuáles de las congruencias

$$x^2 \equiv a \ (mod\ 13)$$

son solucionables cuando a recorre el conjunto $\{1, 2, 3, \dots, 12\}$ módulo 13, los cuadrados de los enteros $1, 2, 3, \dots, 12$ son

$$1^2 \equiv 12^2 \equiv 1 \ (mod\ 13),$$

$$2^2 \equiv 11^2 \equiv 4 \ (mod\ 13),$$

$$3^2 \equiv 10^2 \equiv 9 \ (mod\ 13),$$

$$4^2 \equiv 9^2 \equiv 3 \ (mod\ 13),$$

$$5^2 \equiv 8^2 \equiv 12 \ (mod\ 13),$$

$$6^2 \equiv 7^2 \equiv 10 \ (mod\ 13),$$

Por consiguiente, los residuos cuadráticos de 13 son $1, 3, 4, 9, 10, 12$, mientras que los no residuos son $2, 5, 6, 7, 8, 11$. Observamos que los enteros entre 1 y 12 son divididos igualmente entre los residuos cuadráticos y los no residuos cuadraticos; esta es una característica general.

Euler inventó un criterio simple para decidir si un entero a es un residuo cuadrático de un primo p dado.

Teorema 3.1.2 (Criterio de Euler).

Sea p un primo impar y $mcd(a,p) = 1$. Entonces a es un residuo cuadrático de p si y sólo si

$$a^{(p-1)/2} \equiv 1 \ (mod\ p)$$

Demostración.

"$\Rightarrow$"

Supongamos que a es un residuo cuadrático de p.

Así que

$$x^2 \equiv a \ (mod\ p)$$

admite una solución, llamada x_1.

Ya que $mcd(a,p) = 1$, evidentemente $mcd(x_1,p) = 1$.

Podemos por lo tanto recurrir al Teorema de Fermat para obtener

$$a^{(p-1)/2} \equiv ({x_1}^2)^{(p-1)/2} \equiv {x_1}^{p-1} \equiv 1 \ (mod\ p)$$

"$\Leftarrow$"

En sentido contrario, asumimos que la congruencia

$$a^{(p-1)/2} \equiv 1 \ (mod\ p)$$

es válida, y sea r una raíz primitiva de p.

Entonces

$$a \equiv r^k (mod\ p) \text{ para algún entero } k, \text{ con } 1 \leq k \leq p-1.$$

Se deduce que

$$a^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1\ (mod\ p)$$

Por Teorema 1.4.8, el orden de r (es decir, $p-1$) dividirá al exponente $k(p-1)/2$. La implicación es que k es un entero par, es decir $k = 2j$.

Por consiguiente

$$\left(r^j\right)^2 = r^{2j} = r^k \equiv a\ (mod\ p)$$

Haciendo el entero r^j una solución de la congruencia $x^2 \equiv a\ (mod\ p)$.

Esto prueba que a es un residuo cuadrático del primo p. ■

Ahora si p (como siempre) es un primo impar y $mcd(a,p) = 1$, entonces

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0\ (mod\ p)$$

La última congruencia siendo justificada por el Teorema de Fermat.

Por consiguiente ó $a^{(p-1)/2} \equiv 1\ (mod\ p)$ ó $a^{(p-1)/2} \equiv -1\ (mod\ p)$, pero no ambos. Para que ambas congruencias se dieran simultáneamente, entonces tendríamos $1 \equiv -1\ (mod\ p)$, o equivalentemente $p|2$, lo cual está en conflicto con nuestra hipótesis. Como un residuo no cuadrático de p no satisface $a^{(p-1)/2} \equiv 1\ (mod\ p)$, por lo tanto satisfacerá $a^{(p-1)/2} \equiv -1\ (mod\ p)$. Esta observación mantiene una formulación alterna del Criterio de Euler: el entero a es un residuo no cuadrático del primo *p* si y sólo si $a^{(p-1)/2} \equiv -1\ (mod\ p)$.

Ejemplo 13:

En el caso donde $p = 13$, encontramos que

$$2^{(13-1)/2} \equiv 2^6 \equiv 64 \equiv 12 \equiv -1 \ (mod\ 13).$$

Así, el entero 2 es un residuo no cuadrático de 13.

Como

$$3^{(13-1)/2} \equiv 3^6 \equiv (27)^2 \equiv 1^2 \equiv 1 \ (mod\ 13).$$

El mismo resultado indica que 3 es un residuo cuadrático de 13 y entonces la congruencia

$$x^2 \equiv 3 \ (mod\ 13)$$

es solucionable.

En particular, sus dos soluciones incongruentes son

$$x \equiv 4, 9 \ (mod\ 13).$$

Existe una prueba alternativa del Criterio de Euler (debido a Dirichlet) la cual es más larga, pero quizás más esclarecedora. El razonamiento procede como sigue:

Sea a un residuo no cuadrático de p y sea c uno cualquiera de los enteros $1, 2, 3, \dots, \mathrm{p} - 1$. Por la teoría de congruencias lineales, existe una solución c' de $cx \equiv a \ (mod\ p)$, con c' también en el conjunto $\{1, 2, 3, \dots, \mathrm{p} - 1\}$. Notar que $c' \neq c$, para otro caso tendríamos $c^2 \equiv a \ (mod\ p)$, lo cual contradice lo que asumimos. Así, los enteros entre 1 y $p - 1$ pueden ser divididos en $(p - 1)/2$ pares, c, c', donde $cc' \equiv a \ (mod\ p)$.

Esto lleva a $(p - 1)/2$ congruencias,

$$c_1 c_1' \equiv a \ (mod\ p),$$

$$c_2 c_2' \equiv a \ (mod\ p),$$

$$\vdots$$

$$c_{(p-1)/2}c'_{(p-1)/2} \equiv a\ (mod\ p).$$

Multiplicando ellas juntas y observando que el producto

$$c_1c'_1c_2c'_2 \dots c_{(p-1)/2}c'_{(p-1)/2}$$

es simplemente una reordenación de $1 \cdot 2 \cdot 3 \cdots (p-1)$, obtenemos

$$(p-1)! \equiv a^{(p-1)/2}(mod\ p)$$

En este punto, entra la figura del Teorema de Wilson;

$$(p-1)! \equiv -1\ (mod\ p)$$

Así que

$$a^{(p-1)/2} \equiv -1(mod\ p)$$

El cual es el Criterio de Euler cuando a es un no residuo cuadrático de p.

Corolario 3.1.3

Sea p un primo impar y $mcd(a,p) = 1$. Entonces a es un residuo cuadrático o no residuo cuadrático de p según si

$$a^{(p-1)/2} \equiv 1\ (mod\ p) \quad \text{ó} \quad a^{(p-1)/2} \equiv -1\ (mod\ p).$$

Demostración.

Examinamos el caso en el cual a es un residuo cuadrático de p.

En este caso la congruencia

$$x^2 \equiv a\ (mod\ p)$$

Admite dos soluciones

$x = x_1$ y $x = p - x_1$, para algún x_1 satisfaciendo $1 \leq x_1 \leq p - 1$.

Si x_1 y $p - x_1$ son eliminados del conjunto $\{1, 2, \dots, p-1\}$, entonces los restantes $p - 3$ enteros pueden ser agrupados en pares c, c' (donde $c \neq c'$) talque

$cc' \equiv a \ (mod\ p)$.

Para esas $(p-3)/2$ congruencias, sumar la congruencia

$x_1(p - x_1) \equiv -x_1^2 \equiv -a \ (mod\ p)$.

Tomando el producto de todas las congruencias implicadas llegamos a la relación,

$$(p-1)! \equiv -a^{(p-1)/2} (mod\ p)$$

Nuevamente utilizando el Teorema de Wilson tendremos que

$$-1 \equiv -a^{(p-1)/2} (mod\ p)$$

Y esto implica que

$$a^{(p-1)/2} \equiv 1 \ (mod\ p)$$

Luego, hemos probado que

$$a^{(p-1)/2} \equiv 1 \ (mod\ p) \ \text{ ó } \ a^{(p-1)/2} \equiv -1 \ (mod\ p)$$

De acuerdo a que si a es un residuo cuadrático o no residuo cuadrático de p respectivamente. ■

3.2. Símbolo de Legendre.

Definición 3.2.1

El símbolo de Legendre, (a/p), es una función multiplicativa utilizada en Teoría del Número que toma como argumentos un entero a y un primo p y devuelve uno de los valores 1, -1, ó 0 dependiendo de si a es o no residuo cuadrático módulo p, es decir de si la congruencia

$$x^2 \equiv a \ (mod\ p)$$

tiene o no solución.

Sea p un primo impar y $mcd(a,p) = 1$. El símbolo de Legendre(a/p) es definido por:

$$(a/p) = \begin{cases} 1, & \text{si } a \text{ es un residuo cuadrático de } p. \\ -1, & \text{si } a \text{ no es un residuo cuadrático de } p. \end{cases}$$

Por la terminología tomamos a a como el numerador y a p como el denominador del símbolo (a/p).

Para el caso en que $p|a$ tomamos $(a/p) = 0$.

Teorema 3.2.2

Sea p un primo impar y a y b enteros los cuales son primos relativos a p. Entonces el símbolo de Legendre tiene las siguientes propiedades:

1. Si $a \equiv b \ (mod\ p),\ entonces\ (a/p) = (b/p)$.
2. $(a^2/p) = 1$.
3. $(a/p) \equiv a^{(p-1)/2} \ (mod\ p)$.

4. $(ab/p) = (a/p)(b/p)$.
5. $(1/p) = 1 \ y \ (-1/p) = (-1)^{(p-1)/2}$.

Demostración.

1. Si $a \equiv b \ (mod\ p), \ entonces \ (a/p) = (b/p)$

   Si

   $$a \equiv b \ (mod\ p)$$

   Entonces

   $$x^2 \equiv a \ (mod\ p) \qquad \text{y} \qquad x^2 \equiv b \ (mod\ p)$$

   Tienen exactamente las mismas soluciones, o ninguna.

   Así

   $$x^2 \equiv a \ (mod\ p) \qquad \text{y} \qquad x^2 \equiv b \ (mod\ p)$$

   Es decir a y b son ambos residuos cuadráticos o no lo son, así se tiene que $(a/p) = (b/p)$.

2. $(a^2/p) = 1$

   El entero a satisface la congruencia $x^2 \equiv a^2 \ (mod\ p)$

   Por lo tanto

   $$(a^2/p) = 1.$$

3. $(a/p) \equiv a^{(p-1)/2} (mod\ p)$

   Por el corolario 3.1.3 tenemos que

   $$a^{(p-1)/2} \equiv 1 \ (mod\ p) \qquad \text{o} \qquad a^{(p-1)/2} \equiv -1 \ (mod\ p)$$

   dependiendo si a es o no residuo cuadrático de p, además sabemos que

$$(a/p) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadratico de } p \\ -1 & \text{si } a \text{ no es un residuo cuadratico de } p \end{cases}$$

Sustituyendo 1 por el símbolo de Legendre. De cualquier forma tenemos

$$a^{(p-1)/2} \equiv (a/p)(mod\ p)$$

Por propiedades de congruencia tenemos

$$(a/p) \equiv a^{(p-1)/2}(mod\ p).$$

4. $(ab/p) = (a/p)(b/p)$

$$(ab/p) \equiv (ab)^{(p-1)/2}(mod\ p)$$
$$\equiv (a)^{(p-1)/2}(b)^{(p-1)/2}(mod\ p)$$
$$\equiv (a/p)(b/p)(mod\ p)$$

Ahora el símbolo de Legendre asume sólo los valores de 1 o -1.

Supongamos que existe el caso en que $(ab/p) \neq (a/p)(b/p)$ entonces tendríamos que $1 \equiv -1(mod\ p)$ es decir que $2 \equiv 0(mod\ p)$ lo cual no puede ocurrir ya que $p > 2$. Así tenemos que

$$(ab/p) = (a/p)(b/p).$$

5. $(1/p) = 1\ y\ (-1/p) = (-1)^{(p-1)/2}$.

$(1/p) = 1$. Este es un caso especial de $(a^2/p) = 1$ con $a = 1$

Mientras que

$$(-1/p) = (-1)^{(p-1)/2}$$

es una aplicación de $(a/p) \equiv a^{(p-1)/2}(mod\ p)$ con $a = -1$ es decir

$(-1/p) \equiv (-1)^{(p-1)/2}(mod\ p)$.

Como $(-1/p)\ y\ (-1)^{(p-1)/2}$ son 1 o -1 entonces$(-1/p) \equiv (-1)^{(p-1)/2}$.

El teorema está demostrado. ■

Teorema 3.2.3

Hay infinitos primos de la forma $4k + 1$.

Demostración.

Supongamos que hay primos finitos de esta forma. Llamémosles

$$p_1, p_2, \ \ldots, p_n$$

Y consideremos el entero

$$N = (2p_1p_2 \ \ldots \ p_n)^2 + 1.$$

Es obvio que N es impar, existe algún primo p impar que $p|N$.

Es decir

$$(2p_1p_2 \ \ldots \ p_n)^2 \equiv -1 \ (mod\ p).$$

Escrito en términos del símbolo de Legendre tenemos $(-1/p) = 1$ pero esto sucede solo si p es de la forma $4k + 1$.

Por lo tanto, p es uno de los primos p_i. Esto implica que p_i divide a $N - (2p_1p_2 \ \ldots \ p_n)^2$, o $p_i/1$ lo cual es una contradicción.

Por lo tanto hay infinitos números primos de la forma $4k + 1$. ■

Teorema 3.2.4

Si p es un primo impar, entonces

$$\sum_{a=1}^{p-1}(a\ /\ p) = 0.$$

Por lo tanto, hay precisamente $(p-1)\ /\ 2$ residuos cuadráticos y $(p-1)\ /\ 2$ residuos no cuadráticos de p.

Demostración.

Sea r una raíz primitiva. Sabemos que, módulo p, las potencias $r,\ r^2\ ,\ \ldots\ ,\ r^{p-1}$ son una permutación de los enteros $1, 2,\ \ldots\ ,\ p-1$. Así para cualquier a entre 1 y $p-1$, inclusive, existe un único entero positivo $k\ (1 \leq k \leq p-1)$, tal que $a \equiv r^k (mod\ p)$.

$$\begin{aligned}(a\ /\ p) &= (r^k\ /\ p)\\ &\equiv (r^k)^{(p-1)/2}\\ &= \left(r^{(p-1)/2}\right)^k\\ &\equiv (-1)^k\ (mod\ p).\end{aligned}$$

Como r es una raíz primitiva de p

$$r^{(p-1)/2} \equiv -1\ (mod\ p).$$

Pero $(a\ /\ p)$ y $(-1)^k$ son iguales a 1 o -1, añadiendo el símbolo de Legendre y haciendo la sumatoria de estos tenemos

$$\sum_{a=1}^{p-1}(a/p)\sum_{a=1}^{p-1}(-1)^k = 0.$$

Esto solo puede darse si

$$\sum_{a=1}^{p-1}(a\ /\ p) = 0.$$

Por lo tanto, hay precisamente $(p-1)\ /\ 2$ residuos cuadráticos y $(p-1)\ /\ 2$ residuos no cuadráticos de p. ■

Teorema 3.2.5 (Lema de Gauss)

Sea p un primo impar y sea $mcd(a,p) = 1$. Si n denota el número de enteros en el conjunto

$$S = \left\{a, 2a, 3a,\ \ldots\ , \left(\frac{p-1}{2}\right)a\right\}$$

Cuyos residuos sobre la división por p excede $p/2,$ entonces

$$(a\ /\ p) = (-1)^n$$

Demostración.

Como $mcd(a,p) = 1,$ ninguno de los $(p-1)\ /\ 2$ enteros en S es congruente a cero y no hay dos que sean congruentes entre sí módulo p.

Sean

$$r_1,\ \ldots\ ,\qquad r_m$$

los residuos sobre la división por p tal que $0 < r_i < p/2$ y $s_1,\ \ldots\ , s_n$ los residuos tal que $p > r_i > p/2$.

Entonces $m + n = (p-1)\,/\,2$, y los enteros

$$r_1, \ \ldots \ , r_m, p - s_1, \ \ldots \ , p - s_n$$

son todos positivos y menores que $p/2$.

A fin de demostrar que estos enteros son todos distintos, es suficiente probar que $p - s_i$ no es igual a algún r_j .

Lo hacemos por contradicción, asumimos que

$$p - s_i = r_j$$

para algunos enteros i, y j .

Entonces existen enteros u, v con $1 \leq u, \ v \leq (p-1)/2$, satisfaciendo que

$$s_i \equiv ua \ (mod\ p) \qquad \text{y} \qquad r_j \equiv va \ (mod\ p).$$

Por lo tanto

$$(u+v)a \equiv s_i + r_j \equiv p \equiv 0 \ (mod\ p)$$

De donde tenemos que

$$u + v \equiv 0 \ (mod\ p).$$

Pero esto no puede suceder ya que $1 < u + v \leq p - 1$.

El punto resaltante de esto es que los números $(p-1)/2$ son simplemente los enteros $1, 2, \ \ldots \ , (p-1)/2,$ los cuales no aparecen necesariamente ordenados.

Así tenemos el producto de ellos $[(p-1)/2]!$

$$\left(\frac{p-1}{2}\right)! = r_1 \cdots \ r_m(p - s_1) \ \cdots (p - s_n)$$

$$\equiv r_1 \cdots \ r_m(-s_1) \cdots (-s_n) \ (mod\ p)$$

$$\equiv (-1)^n r_1 \ \cdots \ r_m s_1 \cdots \ s_n \ (mod\ p)$$

Pero sabemos que $r_1, \ldots, r_m, s_1, \ldots, s_n$ son congruentes modulo p a $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a$, en algún orden, de modo que

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a \ (mod\ p)$$

$$\equiv (-1)^n a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \ (mod\ p)$$

Como $\left(\frac{p-1}{2}\right)!$ es primo relativo a p, lo cancelamos de ambos lados de la congruencia y nos da

$$1 \equiv (-1)^n a^{(p-1)/2} \ (mod\ p)$$

Multiplicando por $(-1)^n$ tenemos

$$(-1)^n \equiv (-1)^n (-1)^n a^{(p-1)/2} \ (mod\ p)$$

$$(-1)^n \equiv (-1)^{2n} a^{(p-1)/2} \ (mod\ p)$$

$$(-1)^n \equiv a^{(p-1)/2} \ (mod\ p)$$

$$a^{(p-1)/2} \equiv (-1)^n \ (mod\ p).$$

Usando el criterio de Euler tenemos

$$(a/p) \equiv a^{(p-1)/2} \equiv (-1)^n \ (mod\ p)$$

Lo cual implica que

$$(a/p) = (-1)^n. \qquad \blacksquare$$

Teorema 3.2.6

Si p es un primo impar, entonces

$$(2\ /\ p) = \begin{cases} 1\ si\ p \equiv 1\ (mod\ 8)\ \ o\ \ \ p \equiv 7\ (mod\ 8) \\ -1\ si\ p \equiv 3\ (mod\ 8)\ \ o\ \ \ p \equiv 5\ (mod\ 8) \end{cases}.$$

Demostración.

De acuerdo al teorema de Gauss tenemos, $(2/p) = (-1)^n$, donde n es el número de de enteros en el conjunto

$$S = \left\{2, 2 \cdot 2, 3 \cdot 2,\ \ldots\ , \left(\frac{p-1}{2}\right) \cdot 2\right\}$$

El cual, sobre la división por p, tiene residuos mayores que $p/2$. Los números de S son menores que p, entonces nos basta saber cuántos son los números mayores que $p/2$. Para $1 \leq k \leq (p-1)/2$, $2k < p/2$ si y solo si $k < p/4$. Si [ ] denota la función entero mayor, entonces en S hay $[p/4]$ enteros menores que $p/2$, por lo tanto

$$n = \frac{p-1}{2} - [p/4]$$

Enteros mayores que $p/2$.

Tenemos cuatro posibilidades; cualquier primo impar tiene una de las formas $8k+1,\ 8k+3,\ 8k+5\ o\ 8k+7$.

Calculando tenemos

Si $p = 8k+1$, entonces $n = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k$,

Si $p = 8k+3$, entonces $n = 4k + 1 - \left[2k + \frac{3}{4}\right] = 4k + 1 - 2k = 2k + 1$,

Si $p = 8k+5$, entonces $n = 4k + 2 - \left[2k + 1 + \frac{1}{4}\right] = 4k + 2 - (2k+1) = 2k + 1$,

Si $p = 8k+7$, entonces $n = 4k + 3 - \left[2k + \frac{3}{4}\right] = 4k + 3 - (2k+1) = 2k + 2$.

De donde tenemos que cuando p es de la forma $8k+1\ o\ 8k+7,\ n$ es par y $(2/p)=1$; por otra parte cuando p es de la forma $8k+3\ o\ 8k+5,\ n$ es impar y $(2/p)=-1$. ■

Teorema 3.2.7

Si p y $2p+1$ son ambos primos impares, entonces el entero $(-1)^{(p-1)/2}\cdot 2$ es una raíz primitiva de $2p+1$.

Demostración.

Hagamos $q=2p+1$.

Entonces tenemos dos casos $p\equiv 1\ (mod\ 4)$ y $p\equiv 3\ (mod\ 4)$.

Si

$$p\equiv 1\ (mod\ 4)$$

Entonces

$$p-1=4m \qquad \text{y} \qquad (-1)^{(p-1)/2}\cdot 2=(-1)^{(4m)/2}\cdot 2=2.$$

Como $\phi(q)=q-1=2p,$ el orden de 2 módulo q es uno de los números 1, 2, $p,$ o $2p$.

Del numeral 3) del teorema 3.2.2 tenemos

$$(2/p)=(-1)^{(q-1)/2}=2^p\ (mod\ q)$$

Pero $q\equiv 3\ (mod\ 8);$ donde, $(2/q)=-1.$ Esto muestra que $2^p\equiv -1\ (mod\ q)$ y 2 no puede tener orden p módulo $q.$ El orden de 2 no es 1, 2 ni $p,$ por lo tanto el orden de 2 modulo q es $2p.$ Así 2 es una raíz primitiva de q.

Si

$$p \equiv 3\ (mod\ 4)$$

Entonces

$$p - 3 = 4m \qquad \text{y} \qquad (-1)^{(p-1)/2}2 = (-1)^{(4m+2)/2}2 = -2\,.$$

Y

$$(-2)^p \equiv (-2/q) = (-1/q)(2/q)\ (mod\ q)$$

Como $q \equiv 7\ (mod\ 8)$, del Corolario 2.1.7 tenemos que $(-1/q) = -1$ mientras que una vez más tenemos $(2/q) = 1$.

Esto conduce a la congruencia $(-2)^p \equiv -1\ (mod\ q)$. y -2 es una raíz primitiva de q. ■

3.3. Reciprocidad Cuadrática

Ahora ya estamos listos para enunciar la Ley de Reciprocidad Cuadrática y desarrollar su demostración.

Teorema 3.3.1 (Ley de Reciprocidad Cuadrática)

Si p y q son primos impares distintos, entonces

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

- **Primera Demostración:**

Antes de realizar la primera demostración de La Ley de Reciprocidad Cuadrática (L.R.C.) se introducirá la siguiente notación:

La letra R puesta entre dos cantidades indicará que la primera es un residuo de la siguiente, mientras que la letra N tendrá el significado contrario. Entonces con esta notación la Ley de Reciprocidad Cuadrática queda:

$$pRq \Leftrightarrow qRp \qquad si\ \ p\ o\ q \equiv 1\ (mod\ 4).$$

$$pRq \Leftrightarrow qNp \qquad si\ \ p\ y\ q \equiv -1\ (mod\ 4).$$

Ahora, ya se puede iniciar con la demostración.

Por inducción se puede comprobar que la L.R.C. es válida para números pequeños, de tal manera se determina un límite hasta el cual sea válida.

Ahora, si la L.R.C. no es verdadera en general, existirá algún límite J hasta el cual sea válida, de tal manera que ya no lo sea más para el próximo número mayor que $J + 1$.

Esto es lo mismo que suponer que existen dos números primos, de los cuales el mayor es $J + 1$ y que comparados entre sí contradicen la L.R.C., y además que otros pares cualesquiera de números primos, siendo ambos menores que $J + 1$, cumplen esta ley. Se mostrará que esta suposición es contradictoria, con lo cual se demuestra la Ley de Reciprocidad Cuadrática.

A continuación presentaremos la demostración de los 8 casos generales de la Ley de Reciprocidad Cuadrática.

Primer caso:

Cuando $J+1$ es de la forma $4n+1$ (llamemos a uno de estos números a), y p es de la misma forma, si $\pm pRa$, entonces no puede ser que $\pm aNp$.

Tenemos que $p\ o\ a \equiv 1\ (mod\ 4)$ no se puede dar que $a\ y\ p \equiv -1\ (mod\ 4)$ ya que se llegaría a una contradicción.

Segundo caso:

Cuando $J+1$ es de la forma $4n+1$ (llamemos a uno de estos números a), y p es de la forma $4n+3$, y $\pm pRa$, no puede ser ni $+aNp$ ni $-aRp$.

Tenemos que $a \equiv 1\ (mod\ 4)$ y $p \equiv -1\ (mod\ 4)$ y $-p\ o\ a \equiv 1\ (mod\ 4)$ no se puede dar que ni $a\ y\ p \equiv -1\ (mod\ 4)$ ni $-a\ o\ p \equiv 1\ (mod\ 4)$.

Tercer caso:

Cuando $J+1$ es de la forma $4n+1$ (llamemos a uno de estos números a), y p es de la misma forma y $\pm pNa$, si $\pm pRa$, entonces no puede ser que $\pm aRp$.

Tenemos que $\pm p\ y\ a \equiv -1\ (mod\ 4)$ y que $\pm p\ o\ a \equiv 1\ (mod\ 4)$, no se puede dar que $\pm a\ o\ p \equiv 1\ (mod\ 4)$.

Cuarto caso:

Cuando $J+1$ es de la forma $4n+1$ (llamemos a uno de estos números a), y p es de la forma $4n+3$, y $\pm pNa$, no puede ser ni $+aRp$ ni $-aNp$.

Tenemos que $\pm p\ y\ a \equiv -1\ (mod\ 4)$, no puede darse ni que $a\ o\ p \equiv 1\ (mod\ 4)$ ni que $-a\ y\ p \equiv -1\ (mod\ 4)$.

Quinto caso:

Cuando $J+1$ es de la forma $4n+3$ (llamemos a uno de estos números a), y p es de la misma forma, y $+pRa$ o $-pNa$, no puede ser ni $+aRp$ ni $-aNp$.

Tenemos que $p\ o\ a \equiv 1\ (mod\ 4)$ o $-p\ y\ a \equiv -1\ (mod\ 4)$, no puede darse ni que $a\ o\ p \equiv 1\ (mod\ 4)$ ni que $-a\ y\ p \equiv -1\ (mod\ 4)$.

Sexto caso:

Cuando $J+1$ es de la forma $4n+3$ (llamemos a uno de estos números a), y p es de la forma $4n+1$, y pRa, no puede ser que $\pm aNp$.

Tenemos que $p\ o\ a \equiv 1\ (mod\ 4)$, no puede darse que $\pm a\ y\ p \equiv -1\ (mod\ 4)$.

Séptimo caso:

Cuando $J+1$ es de la forma $4n+3$ (llamemos a uno de estos números a), y p es de la misma forma, y $+pNa$ o $-pRa$, no puede ser ni $+aNp$ ni $-aRp$.

Tenemos que $p\ y\ a \equiv -1\ (mod\ 4)$ o $-p\ o\ a \equiv 1\ (mod\ 4)$, no puede darse ni que $a\ y\ p \equiv -1\ (mod\ 4)$ ni que $-a\ o\ p \equiv 1\ (mod\ 4)$.

Octavo caso:

Cuando $J+1$ es de la forma $4n+3$ (llamemos a uno de estos números a), y p es de la forma $4n+1$, y $+pNa$ o $-pRa$, no puede ser que $\pm aRp$.

Tenemos que $p\ y\ a \equiv -1\ (mod\ 4)$ o $-p\ o\ a \equiv 1\ (mod\ 4)$, pero como $a \equiv -1\ (mod\ 4)$ y $p \equiv 1\ (mod\ 4)$ no puede darse que $\pm a\ o\ p \equiv 1\ (mod\ 4)$.

Demostrados estos casos se da por terminada la prueba de la Ley de Reciprocidad Cuadrática. ■

- **Otra demostración de la Ley de Reciprocidad Cuadrática:**

Considérese el rectángulo en el plano de coordenadas xy cuyos vértices son $(0,0)$, $(\frac{p}{2},0)$, $(0,\frac{q}{2})$ y $(\frac{p}{2},\frac{q}{2})$. Sea R la región dentro de este rectángulo, no incluyendo cualquiera de las líneas que lo limitan. El plan general de la demostración es contar el número de puntos de la red (es decir, los puntos cuyas coordenadas son enteros) en el interior R de dos maneras diferentes. Dado que p y q son ambos impares, los puntos de la red de R se componen de todos los puntos (n,m), donde

$1 \leq n \leq (p-1)/2$ y $1 \leq m \leq (q-1)/2$; el número de estos puntos es claramente

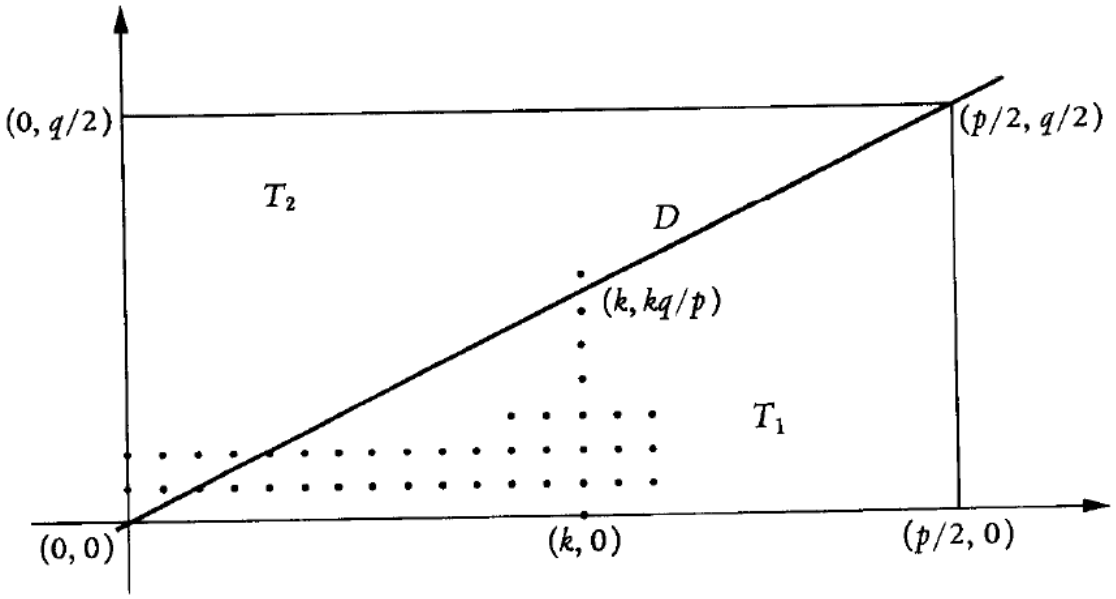
$$\left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right).$$

Ahora la diagonal D a partir de $(0,0)$ a $(p/2, q/2)$ tiene la ecuación $y = (q/p)x$, o de forma equivalente, $py = qx$. Dado que $mcd(p,q) = 1$, ninguno de los puntos de la red dentro de R se encuentran en D. Para p debe dividir la coordenada x de los puntos de la red en la línea de $py = qx$, y q debe dividir la coordenada y, no hay tales puntos en R. Supongamos que T_1 denota la porción de R, que está por debajo de la diagonal D, y T_2 la parte de arriba. Por lo que acabamos de ver, basta con contar los puntos de la red dentro de cada uno de estos triángulos.

El número de números enteros en el intervalo $0 < y < kq/p$ es igual a $[kq/p]$. Por lo tanto, para 1 ≤ *k* ≤ (*p* - 1) / 2, no son precisamente [*kq* / *p*] puntos de la red de

T_1directamente encima del punto (*k*, 0) y por debajo de D, es decir, situada en la vertical segmento de línea desde (*k*, 0) a (*k, kq / p*). De ello se desprende que el número total de puntos de la red que figura en T_1 es

$$\sum_{k=1}^{(p-1)/2} [kq/p]$$



ro

$$\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right) = \sum_{k=1}^{(p-1)/2} [kq/p] + \sum_{j=1}^{(q-1)/2} [jp/q].$$

Es en este momento cuando el Lema de Gauss nos es de mucha utilidad, aplicándolo tenemos

$$(p/q)(q/p) = (-1)^{\sum_{j=1}^{(q-1)/2}[jp/q]} \cdot (-1)^{\sum_{k=1}^{(p-1)/2}[kq/p]}$$

$$= (-1)^{\sum_{k=1}^{(p-1)/2}[kq/p]+\sum_{j=1}^{(q-1)/2}[jp/q]}$$

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

La prueba de la Ley de Reciprocidad Cuadrática ha finalizado. ■

Una consecuencia inmediata de esto es

Corolario 3.3.2

Si p y q son primos impares distintos, y luego

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & si\ \ p \equiv 1(mod\ 4)\ o\ \ q \equiv 1(mod\ 4) \\ -1, & si\ \ p \equiv q \equiv 3(mod\ 4) \end{cases}$$

Corolario 3.3.3

Si p y q son primos impares distintos, y luego

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} (q/p), & si\ \ p \equiv 1(mod\ 4)\ o\ \ q \equiv 1(mod\ 4) \\ -(q/p), & si\ \ p \equiv q \equiv 3(mod\ 4) \end{cases}$$

Veamos lo que lleva a cabo esta última serie de resultados. Tome p como un número primo impar y $a \neq \pm 1$, al ser un número entero no divisible por p. Supongamos, además, que a tiene la factorización

$$a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

cuando el p_i son distintos primos impares. Como se sabe que el símbolo de Legendre es multiplicativo

$$(a/p) = (\pm 1/p)(2/p)^{k_0}(p_1/p)^{k_1} \cdots (p_r/p)^{k_r}.$$

Para evaluar (a/p), sólo tenemos que calcular cada uno de los símbolos $(-1/p)$, $(2/p)$ y (p_i/p). Los valores de $(-1/p)$ y $(2/p)$ se discutieron anteriormente, de modo que el obstáculo es (p_i/p), donde p_i y p son primos impares distintos, que es donde la Ley de Reciprocidad Cuadrática entra.

El Corolario 3.3.2 nos permite reemplazar (p_i/p) por un nuevo símbolo de Legendre tener un denominador más pequeño. A través de la inversión continua y la división, el cálculo se puede reducir a la de las cantidades conocidas $(-1/q)$, $(1/q)$, y $(2/q)$.

3.4 Ejemplos y aplicaciones

La Ley de Reciprocidad Cuadrática nos permite calcular el valor de $\left(\frac{a}{p}\right)$ en muchos casos.

Ejemplo 14

Considere el símbolo de Legendre (29/53).

Así tenemos ambas congruencias

$$29 \equiv 1\ (mod\ 4) \qquad \text{y} \qquad 53 \equiv 1\ (mod\ 4)$$

y vemos que

$$(29/53) = (53/29) = (24/29) = (2/29)\ (3/29)\ (4/29)$$

$$= (2/29)\ (3/29)$$

Con referencia a Teorema 3.2.6, (2/29) = -1

Mientras que invirtiendo otra vez,

$$(3/29) = (29/3) = (2/3) = -1$$

Donde se utilizó la congruencia $29 \equiv 2\ (mod\ 3)$, El efecto es que

$$(29/53) = (2/29)\ (3/29) = (-1)\ (-1) = 1.$$

Ejemplo 15

Otro ejemplo interesante de aplicaciones es el siguiente.

Queremos saber para qué primos, la congruencia $x^2 \equiv 3\ (mod\ p)$ tiene solución. Es decir para que valores de p se tiene que $\left(\frac{3}{p}\right) = 1$.

Desde el 3 ≡ 3 (mod 4), el Corolario 3.3.3 implica que

$$(3/p) = \begin{cases} (p/3) & si \quad p \equiv 1\ (mod\ 4) \\ -(p/3) & si \quad p \equiv 3\ (mod\ 4) \end{cases}$$

Ahora $p \equiv 1\ (mod\ 3)$ o $p \equiv 2\ (mod\ 3)$

Por Teoremas 3.2.2 y 3.2.6,

$$(p/3) = \begin{cases} 1 & si \quad p \equiv 1\ (mod\ 3) \\ -1 & si \quad p \equiv 2\ (mod\ 3)' \end{cases}$$

la implicación de los cuales es que $(3/p) = 1$ si y sólo si

(1) $\qquad p \equiv 1\ (mod\ 4)\ \ y\ p \equiv 1\ (mod\ 3)$,

O

(2) $\qquad p \equiv 3\ (mod\ 4)\ \ y\ p \equiv 2\ (mod\ 3)$.

Las restricciones en congruencias (1) son equivalentes a la exigencia de que $p \equiv 1\ (mod\ 12)$ mientras que los de congruencias (2) son equivalentes a

$p \equiv 11 \equiv -1\ (mod\ 12)$, El resultado de todo esto es:

$$(3/p) = \begin{cases} 1 & si \quad p \equiv \pm 1\ (mod\ 12) \\ -1 & si \quad p \equiv \pm 5\ (mod\ 12) \end{cases}$$

Ejemplo 16

Para un ejemplo de la solución de una congruencia cuadrática con un módulo compuesto, consideraremos

$$x^2 \equiv 196\ (mod\ 1357).$$

Ya que 1357 = 23·59, la congruencia dada es soluble si y sólo si ambos

$$x^2 \equiv 196\ (mod\ 23) \quad y \quad x^2 \equiv 196\ (mod\ 59)$$

son solucionables. Nuestro procedimiento es encontrar los valores de los símbolos de Legendre (196/23) y (196/59).

La evaluación de (196/23) es:

(196/23) = (12/23) = (3/23) = 1.

Por lo tanto, la congruencia $x^2 \equiv 196\ (mod\ 23)$ admite una solución.

En cuanto al símbolo (196/59), la Ley de Reciprocidad Cuadrática permite que escribamos

(196/59) = (19/59) = -(59/19) = -(2/19) = -(-1) = 1.

Por lo tanto, es posible resolver $x^2 \equiv 196\ (mod\ 59)$ y, en consecuencia, la congruencia $x^2 \equiv 196\ (mod\ 1357)$ también.

Para llegar a una solución real, observe que la congruencia $x^2 \equiv 196 \equiv 12\ (mod\ 23)$ se satisface por $x \equiv 9 \cdot 14\ (mod\ 23)$, mientras que $x^2 \equiv 196 \equiv 19\ (mod\ 59)$ tiene soluciones $x \equiv 14 \cdot 45\ (mod\ 59)$. Ahora podemos usar el teorema chino del residuo para obtener las soluciones simultáneas de los cuatro sistemas:

$x \equiv 14\ (mod\ 23)\ \ y\ \ x \equiv 14\ (mod\ 23)$,

$x \equiv 14\ (mod\ 23)\ \ y\ \ x \equiv 45\ (mod\ 59)$,

$x \equiv 9\ (mod\ 23)\ \ y\ \ x \equiv 14\ (mod\ 59)$,

$x \equiv 9\ (mod\ 23)\ \ y\ \ x \equiv 45\ (mod\ 59)$.

Los valores resultantes $x \equiv$ 14, 635, 722, 1343 (mod 1357) son las soluciones deseadas de la congruencia original de $x^2 \equiv 196\ (mod\ 1357)$.

Ejemplo 17

Veamos una aplicación muy diferente de estas ideas. Si $F_n = 2^{2^n} + 1, n > 1$ (Definición 1.5.8), es un primo, entonces 2 no es una raíz primitiva de F_n.

Ahora contamos con los medios para demostrar que el número entero 3 sirve como una raíz primitiva de cualquier primo de este tipo.

Como un primer paso tengamos en cuenta que cualquier F_n es de la forma $12k + 5$. Un argumento simple inductivo confirma que $4^{\mathrm{m}} \equiv 4\ (mod\ 12)$, para $m = 1, 2, \ldots$ ya que $4^{\mathrm{m}} \cdot 4 \equiv 4 \cdot 4\ (mod\ 12)$ y $16 \equiv 4\ (mod\ 12)$ por tanto $4^{\mathrm{m}+1} \equiv 4\ (mod\ 12)$; por lo que debemos tener

$$F_n = 2^{2^n} + 1 = 2^{2m} + 1 = 4^m + 1 \equiv 5\ (mod\ 12)$$

Como F_n es primo de esta forma, el ejemplo 3.4.2 nos permite concluir que

$$(3/F_n) = -1,$$

o, usando el Criterio de Euler,

$$3^{\frac{F_n - 1}{2}} \equiv -1\ (mod\ F_n)$$

El cambio a la phi-función, la última congruencia nos queda

$$3^{\phi(F_n)/2} \equiv -1\ (mod\ F_n)$$

A partir de esto, se puede inferir que el 3 tiene orden $\phi(F_n)$ modulo F_n, y así 3 es una raíz primitiva de F_n.

CONCLUCIÓN

Como pudimos observar a través de este trabajo, fuimos de lo más conocido, definiciones y teoremas básicos en la Teoría Elemental de Números, como los axiomas de suma, de multiplicación y resultados importantes de divisibilidad, luego siguiendo un camino a través de la teoría de congruencias, sus propiedades, también abordando las congruencias lineales y algunos resultados importantes y necesarios para el desarrollo de este documento.

Se desarrolló lo que son las congruencias cuadráticas con módulo primo y el Criterio de Euler para residuos cuadráticos, luego pudimos observar el símbolo de Legendre y sus propiedades, para terminar con un bosquejo de la primera demostración de La Ley de Reciprocidad Cuadrática y otros resultados a partir de esta ley, y también pudimos desarrollar aplicaciones mediante algunos ejemplos.

Podemos concluir este trabajo afirmando que La Ley de Reciprocidad Cuadrática es un resultado notable que proporciona un método práctico para determinar el carácter cuadrático de un número, nos ayuda a determinar la solubilidad de las congruencias cuadráticas, también a calcular símbolos de Legendre de una forma más sencilla y hasta poder ver si un número es raíz primitiva de un primo.

BIBLIOGRAFIA

1. Elementary Number Theory - David M. Burton – University of New Hampshire, 1976.

2. Introducción a la Teoría de Números Ejemplos y Algoritmos - Walter Mora F – Instituto Tecnológico de Costa Rica.

3. Introducción a la Teoría de los Números - Niven y Zuckerman.

4. http://web.uam.es/personal_pdi/ciencias/cillerue/Curso/capitulo%204.pdf.

5. http://www.saber.ula.ve/bitstream/123456789/15962/1/reciprocidad.pdf.

6. http://www.accefyn.org.co/grupos/ArchivosIgusa/Martinez_Caro.pdf.