Introducción a la TEORÍA DE NÚMEROS

Rita Roldán Inguanzo

$$M_{82589933} = 2^{82589933} - 1$$

$$6, 28 \quad F_n = 2^{2^n} + 1$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34$$

$$M_n = 2^n - 1$$

$$(3,5), (5,7), (11,13)$$

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

$$(220, 284)$$

EDUNIV Editorial Universitaria

INTRODUCCIÓN A LA TEORÍA DE NÚMEROS

RITA ROLDÁN INGUANZO

Facultad de Matemática, Universidad de La Habana, 2022

EDUNIV
Editorial Universitaria

510-R744 2022
Roldán Inguanzo, Rita

Introducción a la teoría de números / Rita Roldán Inguanzo; Universidad de La Habana. Facultad de Matemática. – La Habana : Editorial Universitaria, 2022. – ISBN: 978-959-16-4727-6 (PDF interactivo). – (vi, 309 páginas): ilustraciones. – 8,5 por 11,0 pulgadas.

1. Matemática; 2. Universidad de La Habana. Facultad de Matemática
I. Título.

Disponible en http://www.eduniv.cu

Disponible en http://www.elibro.com

Rita Alejandra Roldán Inguanzo (La Habana, 1962).

Graduada de Licenciatura en Matemática en la Universidad Friedrich Schiller de Jena en Alemania. Con más de 30 años como profesora de MATCOM, UH; preside actualmente la Comisión Nacional de la carrera de Matemática y coordina la mención de *Análisis Matemático y Álgebra* de la Maestría en Ciencias Matemáticas de su facultad. Es profesora titular de MATCOM y metodóloga de la Dirección de Formación de Pregrado de la Universidad de La Habana (UH). Ha publicado varios libros y numerosos artículos científicos en Cuba y en el extranjero. Impartió junto a otro profesor el curso televisivo *Números y Figuras en la Historia* en Universidad para todos. Es la representante de Cuba en la Olimpiada Iberoamericana de Matemática Universitaria y coordina la Olimpiada Nacional Universitaria de Matemática. Es poseedora del Premio de tercera categoría de la **Universidad Friedrich Schiller de Jena**, de la Distinción por la Educación Cubana y obtuvo el premio Raimundo *Reguera* que otorga la Sociedad Cubana de Matemática y Computación

ÍNDICE

A MODO DE INTRODUCCIÓN

La Teoría de Números ha ocupado siempre una posición básica en la Matemática. No se puede cuestionar su importancia histórica, como una de las pocas áreas de la Ciencia con resultados anteriores a la idea de toda universidad o academia. Nacida en la antigüedad clásica, la Teoría de Números, ha sido testigo de manera prácticamente continua de nuevos y fascinantes descubrimientos relativos a las propiedades de los números y, en cierto punto de sus carreras, la mayoría de los grandes maestros de la Ciencia Matemática han contribuido a este cuerpo de conocimiento.

Es así que la Teoría de Números resulta muy atractiva no solo para los matemáticos sino también para los aficionados a esta ciencia. Sus problemas parecen sencillos y fáciles de resolver (sin necesidad de disponer de conocimientos matemáticos profundos) a primera vista, y la mayoría son incluso muy bonitos, pero... el camino a su solución puede estar lleno de escollos. Muchos de los problemas de apariencia tan sencilla se han resistido a los ataques intelectuales por años y se suman a la lista de los problemas abiertos en la Matemática.

La Teoría Elemental de los Números pudiera ser, en nuestra opinión, un tema clave para iniciarse en el mundo del aprendizaje de la Matemática. No se necesita una fuerte preparación previa y los temas son de fácil comprensión, además de ser básicos para el estudio posterior de la Matemática. Sus métodos de trabajo, con fuerte base en la intuición, la realización de muchos intentos de prueba y error y la experimentación paciente y laboriosa previa a la demostración rigurosa, imitan a los de la investigación científica. No deja de asombrar el hecho del alto número de matemáticos famosos que han dedicado su intelecto al tránsito por el sinuoso camino de la resolución de problemas de la Teoría de Números.

No faltan quienes opinan que la Teoría de Números es un área estéril, un tema limítrofe de la Matemática y su valor solo se expresa en su belleza. Nada es más lejano de la realidad. En la actual era de las tecnologías de la información y la comunicación, los números primos son los soldados imprescindibles de toda comunicación segura. Su historia muestra además la continuidad y actualidad de su desarrollo alimentado por el esfuerzo de sus practicantes, que a menudo significó siglos de trabajo continuo para obtener resultados significativos.

El curso de Teoría de Números que se oferta en la Facultad de Matemática y Computación de la Universidad de La Habana intenta presentar el tema en su relación más básica con las disciplinas de Álgebra y Análisis Matemático.

El texto que a continuación se presenta, pretende ser el material básico para dicho curso. Se presupone que el estudiante dispone de ciertos conocimientos básicos, como son los relativos a las propiedades de los números naturales, enteros, racionales y reales, el método de la inducción completa y la teoría de divisibilidad. Asímismo, son necesarios los conocimientos básicos de las disciplinas de Álgebra y Análisis Matemático. Sin embargo, gran parte del texto también puede ser estudiada por estudiantes interesados de nivel preuniversitario, para los cuales los capítulos 1 al 3 y una adecuada selección de los capítulos 5 y 6 pudieran constituirse en la base de un curso bastante completo.

En el libro se presentan además algunos de los más interesantes problemas abiertos de la Teoría Aritmética de los Números y se incluye un listado bastante amplio de ejercicios, muchos de los cuales han sido seleccionados de la bibliografía referenciada al final del este texto. Complementa el material la presentación de notas biográficas e históricas que pretenden darle una imagen más vivencial.

La autora pone en sus manos un texto susceptible de mejoras, por lo que agradece de antemano todo comentario o sugerencia respecto al mismo en su conjunto o a espacios particulares en él.

Muchas Gracias

La autora (e-mail: rroldan@matcom.uh.cu)

Capítulo 1

LOS CIMIENTOS

1.1. Sobre el origen de la Teoría de Números

La Matemática cuentra entre sus más antiguas ramas a la Teoría de Números. Es probable que fueran los babilónicos y los antiguos egipcios, antes que los griegos, los primeros en estudiar las propiedades de los números naturales, pero es a Pitágoras y sus discípulos a quienes los historiadores acreditan los primeros rudimentos de una Teoría de Números.

Aunque es quizás el matemático más popular de la Antigüedad, es muy poco lo que se conoce de la vida de Pitágoras. Se estima que nació entre 580 y 562 A.C. en la isla egea de Samos y se asume que estudió en Egipto y en la lejana Babilonia, para establecerse finalmente en Crotona, Grecia, donde fundó su famosa escuela.

La escuela pitagórica enseñaba las siete artes consideradas esenciales para la educación de una persona: el *trivium* de lógica, gramática, y retórica y el *quadrivium* conformado por la *arithmetica* (la aritmética, en el sentido de teoría del número, en lugar del arte de calcular), *harmonia* (la música), *geometria* (la geometría) y *astrologia* (la astronomía).

Los asistentes a las conferencias de Pitágoras se dividían en dos grupos: los principiantes (u oyentes) y los pitagóricos. Los pitagóricos constituían una estrecha hermandad, donde consideraban los bienes mundanos comunes a todos, mientras que un juramento prohibía revelar los secretos del fundador. Es así que con el tiempo se constituyen en una sociedad filosófica y matemática, en la que se mantiene el orden confidencial, no publicaban nada y atribuían todos sus descubrimientos al Maestro. Los pitagóricos creían que la clave para una explicación del universo se basaba en el número y su tesis general era "*Todo es número*", entendiendo por número a todo entero positivo. Tal tesis se basaba en la creencia de la conmensurabilidad de todos lo segmentos.

El misticismos de la doctrina pitagórica asignaba a todo objeto, material o espiritual,

un entero definido. Así, por ejemplo, el 1 representaba la razón, pues la razón podría producir sólo un cuerpo consistente de verdades, el 2 simbolizaba al hombre y el 3 a la mujer; el 4 era el símbolo pitagórico de la justicia, por ser el primer número que es el producto de iguales; el 5 se relacionaba con el matrimonio, pues se forma por la unión de 2 y 3; y así sucesivamente. Todos los números impares (excepto el 1) eran considerados como lo femenino y la tierra, y eran poco valorados. Como sociedad predominantemente masculina, clasificaron a los números pares como lo masculino y divino.

Fue en Alejandría y no en Atenas, donde primero comenzó a desarrollarse una ciencia de números que no se apoyaba en la filosofía mística. Durante casi mil años, hasta su destrucción por los árabes en 641 D.C., Alejandría fue considerada el centro cultural y comercial del mundo de helenístico. Después de la caída de Alejandría, la mayoría de sus estudiosos emigró a Constantinopla, donde se conservó para la actualidad el trabajo matemático de las escuelas griegas. El llamado Museo de Alejandria, un precursor de la universidad moderna, reunió a los principales poetas y estudiosos del momento. Adyacente a él se estableció una enorme biblioteca, famosa por conservar mas de 700,000 volumenes-manuscritos. Entre todos los nombres distinguidos relacionados con el museo, el de Euclides (aprox. 350 A.C.), fundador de la Escuela de Matemática y cuyo nombre se asocia generalmente a la Geometría, ocupa un lugar primario. Su obra cumbre "Elementos" es el tratado griego más antiguo en la Matemática, que recopiló gran parte del conocimiento matemático de la época en trece libros, de los cuales los Libros, VII, VIII, IX, se dedican a la Teoría de Números. Se dice que "Elementos" de Euclides constituye uno de los grandes éxitos de la literatura mundial y es el segundo libro más publicado después de La Biblia, con más de mil ediciones desde la primera versión impresa en 1482, y aún se utiliza para la enseñanza de la Matemática en Europa Occidental.

Algunos famosos estudiosos de la Teoría de Núumeros en la historia que aparecerán en este texto son: Pitágoras(569-500 A.C.), Euclides (ca. 350 A.C.), Erathostenes (276-196 A.C.), Nicomachus (ca. 100), Diofanto (ca. 250), Claude Bachet (1581-1638), Marin Mersenne (1588-1648), Pierre de Fermat (1601-1665), Bernard Frenicle de Bessy (1605-1670), Gottfried Leibniz (1646-1716), Christian Goldbach (1690-1764), Leonhard Euler (1707-1783), Edward Waring (1734-1798), Joseph Louis Lagrange (1736-1813), John Wilson (1741-1793), Adrien Marie Legendre (1752-1833), Carl Friedrich Gauss (1777-1855), Augustus Moebius (1790-1868), Karl Gustav Jacobi (1804-1851), Peter Gustav Dirichlet (1805-1859), Joseph Liouville (1809-1882), P. L. Tchebychef (1821-1894), Leopold Kronecker (1823-1891), Edouard Lucas (1842-1891), David Hilbert(1862-1943), Charles de la Vallee Poussin (1866-1962), Chen Jingrun (1933-1996), Ivan Vinogradov (1891-1983), Paul Erdös (1913-199), Atle Selberg (1917-2007), entre muchos otros.

1.2. Los números enteros

La Teoría de Números se relaciona, al menos en sus aspectos elementales, con las propiedades de los números enteros, en particular de los enteros positivos $1, 2, 3, \ldots$ (conocidos también como números naturales). El origen de esa denominación se remonta a la antigua Grecia, donde la palabra "número" significaba entero positivo y nada más. Es famosa la frase del matemático Kronecker[1], quien afirmó que

"*Dios creó los números [naturales], el resto es obra del hombre.*"

Pero, lejos de ser una dádiva del cielo, la Teoría de Números ha tenido una larga y en ocasiones penosa evolución. Sin pretender construir axiomáticamente los números enteros, se presenta aquí una serie de propiedades básicas de dicho conjunto $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, que serán consideradas como axiomas sobre los que se erige la Teoría Elemental de los Números.

(i) Si a, b son enteros entonces $a + b$, y ab también lo son. (**Cerradura de** $\mathbb{Z}$)

(ii) Para cualesquiera enteros a, b es $a + b = b + a$, $ab = ba$. (**Ley Conmutativa**)

(iii) Para cualesquiera enteros a, b, c es $(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$. (**Ley Asociativa**)

(iv) Para cualesquiera enteros a, b, c es $(a + b)c = ac + bc$. (**Ley Distributiva**)

(v) Para cualquier entero a es $a + 0 = a$, $a(1) = a$. (**Elementos neutros**)

(vi) Para todo entero a existe una solución entera de la ecuación $a + x = 0$. Esta solución se conoce como **inverso aditivo** de a y se denota por $-a$. La expresión $b - a$ significa $b + (-a)$.

(vii) Si a, b, c son enteros tales $ac = bc$ y c es no nulo, entonces $a = b$. (**Ley de cancelación**)

EJEMPLO: Utilizando las propiedades anteriores se demuestra que $a \cdot 0 = 0$.

Demostración: Para la demostración se parte de la igualdad $0+0 = 0$. Al multiplicar por el entero a se obtiene

$$(0 + 0) \cdot a = 0 \cdot a + 0 \cdot a = 0 \cdot a,$$

de donde se deduce que $0 \cdot a = 0$. **Q.e.d.**

Muchas de las propiedades más interesantes de los números enteros se deducen a partir de la existencia de un orden en ese conjunto.

[1]Leopold Kronecker (1823-1891)

DEFINICIÓN 1.2.1

Si $a, b \in \mathbb{Z}$ se dice que a ***es menor (mayor) que*** *b, y se denota $a < b$ ($a > b$), si $b - a$ es un número positivo (negativo).*

Note que a es un número positivo si y sólo si $a > 0$ y se cumplen las propiedades siguientes.

(viii) Para cualesquiera enteros positivos a, b se cumple que $a + b$ y ab son también enteros positivos. (**Cerradura de $\mathbb{Z}_+$**)

(ix) Para todo entero a, siempre se cumple $a > 0$, $a < 0$, ó $a = 0$. (**Ley de tricotomía**)

Esta última propiedad permite afirmar que el conjunto de los números enteros es un **conjunto ordenado**.

EJEMPLO: Si $a < b$, entonces $b - a > 0$. Al multiplicar por c se obtiene que $(b - a)c = bc - ac > 0$, de donde se deduce que $ac < bc$.

(x) Todo conjunto no vacío de enteros positivos tiene un menor elemento (**Principio del buen orden.**)

A partir de esta última propiedad se dice que el conjunto de los números enteros positivos ($\mathbb{Z}_+$) está **bien ordenado**.

Sin embargo, el conjunto $\mathbb{Z}$ de todos los números enteros no está bien ordenado, pues existen subconjuntos suyos que no tienen un menor elemento. Por otra parte, se puede comprobar el conjunto de los números enteros menores o iguales a un entero dado tiene un mayor elemento (aplique el principio del buen orden para demostrarlo).

DEFINICIÓN 1.2.2

Se define como parte entera *de un número real x (Notación $[x]$) al mayor entero menor o igual a x, es decir, $[x] \leq x < [x] + 1$.*

EJEMPLO: $\left[\frac{5}{2}\right] = 2$, $\left[-\frac{5}{2}\right] = -3$, $[\pi] = 3$, $[-2] = -2$, $[0] = 0$.

A continuación se utiliza el principio del buen orden para demostrar una propiedad esencial de los números enteros positivos (que se extiende a los números racionales y reales).

TEOREMA 1.2.1

Propiedad arquimediana

Si a y b son enteros positivos, entonces existe un entero positivo n tal que $na \geq b$.

Demostración: Supongamos que no se cumple la propiedad arquimediana, es decir, que existen enteros a y b tales que $na < b$ para todo entero positivo n. Entonces el conjunto

$$S = \{b - na;\ n \in \mathbb{Z}_+\}$$

consiste totalmente de enteros positivos. Por el principio del buen orden S tiene un menor elemento al que llamaremos $b - ma$. Pero $b - (m+1)a$ también pertenece a S, dado que S contiene a todos los enteros de esa forma. Como $b - (m+1)a < b - ma$ se produce una contradicción, lo que demuestra el teorema. **Q.e.d.**

Una interesante aplicación del principio del buen orden, es la demostración de la irracionalidad de ciertos números. Recordemos que un número real es **racional** si se puede expresar como cociente de dos números enteros y es **irracional** en caso contrario. Mediante el principio del buen orden se demuestra de manera sencilla la irracionalidad de $\sqrt{2}$.

Demostración: Supongamos que $\sqrt{2}$ es un número racional, de modo que existen enteros a, b (con $b \neq 0$) tales que

$$\sqrt{2} = \frac{a}{b}.$$

Entonces el conjunto

$$S = \left\{k\sqrt{2}; k \text{ y } k\sqrt{2} \text{ son enteros positivos}\right\}$$

es un conjunto no vacío de enteros positivos (no vacío pues $a = b\sqrt{2}$ es elemento de S) y la propiedad del buen orden garantiza la existencia de un menor elemento en S. Sea éste $s = t\sqrt{2}$.

Entonces $s\sqrt{2} - s = (s-t)\sqrt{2}$ es un número entero, pues $s\sqrt{2} = 2t$ y s son enteros. Además $(s-t)\sqrt{2}$ es positivo, pues $s\sqrt{2} - s = s(\sqrt{2}-1)$ y $\sqrt{2} > 1$. Luego $(s-t)\sqrt{2} \in S$.

Pero $(s-t)\sqrt{2} < s$ (pues $s\sqrt{2} = 2t, s = t\sqrt{2}$ y $\sqrt{2} < 2$), lo cual es imposible, puesto que s es el menor elemento de S. **Q.e.d.**

1.2.1. Ejercicios

1. Demuestre que el conjunto de los números enteros negativos no es bien ordenado.

2. Demuestre que el conjunto de los números racionales positivos no es bien ordenado.

3. Demuestre que el conjunto S es bien ordenado si:

a) $S = \{x \in \mathbb{Z} : x > 3\}$

b) $S = \{x \in \mathbb{Q} : x = \frac{a}{2}, a \in \mathbb{Z}^+\}$

4. Demuestre que cualquier conjunto de números enteros negativos tiene un mayor elemento.

5. Demuestre que el conjunto de los enteros menores o iguales a un entero dado tiene un mayor elemento.

6. Halle a) $[21.2]$ b) $\left[\frac{1}{7}\right]$ c) $[\sqrt{3}]$ d) $[-\pi]$

7. Demuestre que si x es un número real cualquiera, entonces

$$[x + k] = [x] + k$$

para todo valor entero de k.

8. Demuestre que si x, y son números positivos reales cualesquiera, entonces $[xy] \geq [x][y]$.

9. Halle $[x] + [-x]$ para x real.

10. Demuestre que si x es es un número real no negativo cualquiera, entonces

$$[x] + \left[x + \frac{1}{2}\right] = [2x].$$

11. Responda verdadero o falso según corresponda. Justifique su respuesta

a) La suma de un número irracional y uno racional es irracional.

b) La suma de dos números irracionales es irracional.

c) El producto de un número irracional y uno racional es irracional.

d) El producto de dos números irracionales es irracional.

12. Demuestre que $\sqrt{3}$ es un número irracional.

13. Demuestre que si $a_k \in \mathbb{R}$ para todo valor entero no negativo de k menor o igual a n, entonces es

$$\sum_{k=1}^{n} (a_k - a_{k-1}) = a_n - a_0.$$

14. Calcule $\sum_{k=1}^{n} \frac{1}{k(k+1)}$.

1.3. Inducción matemática

A partir del principio del buen orden resulta sencillo derivar el primer principio de indución matemática, que constituye una poderosa herramienta para la demostración de propiedades de conjuntos de números enteros. La esencia de dicho principio se puede ejemplificar en un juego que muchos desarrollábamos en edades tempranas, cuando ordenábamos las fichas de dominó "paradas" en una fila para luego derribarlas todas de sólo un golpe a la primera ficha. La idea que está detrás de ese juego es la siguiente: cuando dos fichas de dominó se colocan paradas lo suficientemente cerca, entonces al tumbar una se cae la otra al ser empujada por la primera; luego si las ordenamos todas bien pegaditas, basta tumbar la primera para que caigan todas. A continuación se presenta el primer principio de la inducción matemática.

TEOREMA 1.3.1 ***El primer principio de la inducción matemática***

Sea S un conjunto de enteros positivos que cumple las siguientes propiedades:

(1) $1 \in S$

(2) si $n \in S$*, entonces* $n+1 \in S$*.*

Entonces S es el conjunto de todos los enteros positivos $\mathbb{Z}_+$.

Demostración: Sea S un conjunto de enteros positivos con las propiedades (1) y (2). Es obvio que $S \subset \mathbb{Z}_+$.

Sea $T = \mathbb{Z}_+ \setminus S$ el conjunto de todos los enteros positivos que no son elementos de S. Por el principio del buen orden, T posee un menor elemento, al que llamaremos a. Como $1 \in S$, obviamente tiene que ser $a > 1$, por lo que $0 < a-1 < a$. Como a es el menor elemento de T, entonces $a-1 \notin T$, es decir, $a-1 \in S$. Pero la condición (2) implica entonces que $a \in S$, lo que constituye una contradicción. Luego tiene que ser $T = \emptyset$, o lo que es lo mismo, $S = \mathbb{Z}_+$. **Q.e.d.**

Para demostrar una propiedad de los números enteros mediante el principio de la inducción matemática se necesitan seguir tres pasos, a saber:

i) *Paso Básico*: Demostrar que la propiedad se cumple para $n = 1$ (o para el primer elemento del conjunto en cuestión).

ii) *Hipótesis de Inducción*: Suponer que la propiedad se cumple para un entero n cualquiera.

iii) *Paso Inductivo*: Demostrar que entonces la propiedad se cumple para $n+1$.

EJEMPLO: Compruebe la veracidad de la conocida fórmula

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

a través del primer principio de la inducción matemática.

Demostración:

i) *Paso Básico*: Para $n = 1$ se cumple la fórmula, pues

$$1^2 = 1 = \frac{1(2)(3)}{6}.$$

ii) *Hipótesis de Inducción*: Supongamos que la fórmula se cumple para un entero n, es decir

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

iii) *Paso Inductivo*: Se desea demostrar que la fórmula se cumple para $n+1$, es decir, que se cumple

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \ldots + n^2 + (n+1)^2 &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}. \end{aligned}$$

Al grupar convenientemente los sumandos en el miembro izquierdo y aplicar la hipótesis de inducción se obtiene

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \ldots + n^2 + (n+1)^2 &= \left[1^2 + 2^2 + 3^2 + \ldots + n^2\right] + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)[n(2n+1) + 6(n+1)]}{6} \\ &= \frac{(n+1)(2n^2+7n+6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}, \end{aligned}$$

que es lo que se quería demostrar. **Q.e.d.**

Mientras la inducción matemática resulta ser una técnica estándar para demostrar propiedades sobre números enteros, tiene la curiosa desventaja de no indicar cómo formular (o inducir) esas propiedades. A pesar de lo que su nombre indica, la inducción matemática es realmente un método deductivo de demostración. Por supuesto, si después una reflexión más o menos larga, se supone (se induce) la propiedad que se desea demostrar, entonces la inducción matemática puede ser una herrameinta realmente efectiva para lograrlo. Obvia decir que no hay camino trillado para lograr una conjetura, sólo la experiencia puede ayudar en ese sentido. Veamos un ejemplo:

EJEMPLO: Calcule $1+3+5+\cdots+(2n-1)=\sum_{k=1}^{n}(2k-1)$.

Para conjeturar una fórmula se prueba con los primeros valores de n.

$$\begin{aligned} 1 &= 1 = 1^2 \\ 1+3 &= 4 = 2^2 \\ 1+3+5 &= 9 = 3^2 \\ 1+3+5+7 &= 16 = 4^2 \\ 1+3+5+7+9 &= 25 = 5^2 \\ 1+3+5+7+9+11 &= 36 = 6^2. \end{aligned}$$

En este caso parece ser que siempre se van obteniendo los cuadrados de los números enteros positivos. Así se propone la conjetura:

$$\sum_{k=1}^{n}(2k-1)=n^2.$$

Demostración:

i) $\sum_{k=1}^{1}(2k-1)=1=1^2$, por lo que la conjetura es válida para $n=1$.

ii) Sea $\sum_{k=1}^{n}(2k-1)=n^2$.

iii) Se desea probar que $\sum_{k=1}^{n+1}(2k-1)=(n+1)^2$. Al desarrollar a partir del miembro izquierdo se obtiene

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

Q.e.d.

Las progresiones geométricas juegan un importante papel en la teoría.

DEFINICIÓN 1.3.1

Una ***progresión geométrica*** *es una sucesión de la forma*

$$a, ar, ar^2, ar^3, \ldots,$$

donde a, r *son números reales y* $r \neq 1$.

La suma de la progresión geométrica cumple:

$$\sum_{k=0}^{n} ar^k = \frac{ar^{n+1} - a}{r-1} = a\frac{r^{n+1}-1}{r-1}.$$

Demostración:

i) $\sum_{k=0}^{1} ar^k = a + ar = a(1+r) = \frac{a(r+1)(r-1)}{(r-1)} = a\frac{r^2-1}{r-1}$.

ii) Sea $\sum_{k=0}^{n} ar^k = a\frac{r^{n+1}-1}{r-1}$.

iii) Se desea demostrar que $\sum_{k=0}^{n+1} ar^k = \frac{ar^{n+2}-a}{r-1}$.

$$\begin{aligned}\sum_{k=0}^{n+1} ar^k &= \sum_{k=0}^{n} ar^k + ar^{n+1} = a\frac{r^{n+1}-1}{r-1} + ar^{n+1} \\ &= a\left(\frac{r^{n+1} - 1 + r^{n+2} - r^{n+1}}{r-1}\right) \\ &= a\frac{r^{n+2}-1}{r-1}.\end{aligned}$$

Q.e.d.

Esta fórmula es muy útil para calcular sumas interesantes. Por ejemplo:

$$\sum_{k=0}^{n} 2^k = \frac{2^{n+1}-2}{2-1} = 2^{n+1} - 1.$$

Nótese que en estos ejemplos no se ha mencionado al conjunto S y se ha procedido comprobando simplemente *las dos* propiedades que caracterizan al principio de inducción matemática. En este sentido se debe sumamente cuidadoso de no olvidar comprobar el resultado a demostrar para el primer elemento del conjunto. No hacerlo sería como ordenar las filas del dominó correctamente y no hacer caer la primera ficha,..., por supuesto, que en ese caso no caería ninguna más. No demostrar la tesis de inducción a partir de la hipótesis de inducción sería como colocar las

fichas demasiado separadas entre sí. La validez de la tesis de inducción no depende únicamente de la veracidad de la hipótesis de inducción. Por ejemplo, según lo anteriormente demostrado es obvio que la siguiente fórmula es falsa

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 + 3.$$

Sin embargo, si se asume que la fórmula es válida para un entero n, entonces para $n + 1$ se tiene

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) &= [1 + 3 + 5 + \cdots + (2n - 1)] + (2n + 1) \\ &= [n^2 + 3] + (2n + 1) \\ &= (n^2 + 2n + 1) + 3 \\ &= (n + 1)^2 + 3, \end{aligned}$$

por lo que la fórmula sería válida para $n + 1$. Pero para completar la demostración faltaría comprobar para un primer elemento, lo cual no será posible en este ejemplo particular.

Una segunda variante del principio de inducción matemática puede resultar de gran utilidad cuando el primer principio parece poco efectivo.

TEOREMA 1.3.2 ***El segundo principio de inducción matemática***

Si un conjunto de enteros positivos contiene al 1 *y cumple la propiedad de que para cada entero positivo* n*, si contiene a todos los enteros menores o iguales que* n*, contiene a* $n + 1$*, entonces se trata del conjunto de todos los enteros positivos* $\mathbb{Z}_+$.

La demostración de este teorema es muy sencilla y queda como ejercicio para el lector.

Normalmente se utiliza más el primer principio de inducción matemática que el segundo, pero existen ocasiones, donde sólo es posible usar el último.

EJEMPLO: Demuestre que todo franqueo postal de valor mayor que 1 centavo, puede ser formado utilizando solamente sellos de 2 y 3 centavos.

Demostración: Es obvio que la afirmación es válida para los franqueos de 2 y de 3 centavos y supongamos que también lo es para franqueos de hasta n centavos. El franqueo de $n + 1$ centavos se puede conformar con el franqueo de $n - 1$ centavos (el cual cumple la hipótesis de inducción y contiene solamente sellos de 2 y 3 centavos) y un sello de 2 centavos. Queda así demostrada la afirmación. **Q.e.d.**

El principio de inducción matemática sugiere un método para definir funciones en los enteros positivos. En lugar de definir explícitamente el valor de la función se define el valor de $f(1)$ y se ofrece un regla para calcular $f(n + 1)$ a partir del valor de $f(n)$.

DEFINICIÓN 1.3.2

*Se dice que la función f esta **definida recursivamente** si se especifica el valor de $f(1)$ y una regla para determinar $f(n+1)$ a partir de $f(n)$.*

EJEMPLO: La función factorial $f(n) = n!$ se define recursivamente como

i) $f(1) = 1$,

ii) $f(n+1) = (n+1)f(n)$.

EJEMPLO: Este ejemplo relaciona la definición recursiva con la demostración a través del segundo principio de inducción matemática. La sucesión de Lucas[2]

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$$

se define recursivamente como

$$a_1 = 1, \quad a_2 = 3, \quad a_n = a_{n-1} + a_{n-2} \quad \text{para todo } n \geq 3.$$

A continuación se demuestra que para todo entero positivo n se cumple la desigualdad

$$a_n < \left(\frac{7}{4}\right)^n.$$

Como la definición recursiva del término n-ésimo de la sucesión depende de los dos términos anteriores, resulta claro que será necesario aplicar el segundo principìo de inducción para demostrar la desigualdad.

Demostración:

i) Para $n = 1$ y $n = 2$ se tiene

$$a_1 = 1 < \left(\frac{7}{4}\right)^1 = \frac{7}{4},$$

$$a_3 = 3 < \left(\frac{7}{4}\right)^2 = \frac{49}{16}.$$

ii) Sea válida la desigualdad para todo entero positivo menor que n, es decir

$$a_k < \left(\frac{7}{4}\right)^k \quad \text{para todo } k = 1, \ldots, n-1.$$

[2]Edouard Lucas (1842-1891)

iii) Se desea demostrar la desigualdad para n, es decir, que

$$a_n < \left(\frac{7}{4}\right)^n.$$

Aquí se cumple

$$\begin{aligned} a_n = a_{n-1} + a_{n-2} &< \left(\frac{7}{4}\right)^{n-1} + \left(\frac{7}{4}\right)^{n-2} \\ &= \left(\frac{7}{4}\right)^{n-2}\left(\frac{7}{4}+1\right) = \left(\frac{7}{4}\right)^{n-2}\left(\frac{11}{4}\right) \\ &< \left(\frac{7}{4}\right)^{n-2}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^n, \end{aligned}$$

que es lo que se quería demostrar. **Q.e.d.**

1.3.1. Ejercicios

1. Demuestre que:
   a) $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$ para todo $n \geq 1$.
   b) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + n(n+1) = \frac{n(n+1)(n+2)}{3}$ para todo $n \geq 1$.
   c) $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{n(4n^2-1)}{3}$ para todo $n \geq 1$.
   d) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ para todo $n \geq 1$.

2. Demuestre que para todo $n \geq 1$ se cumple
$$a^n - 1 = (a-1)(a^n + a^{n-1} + \ldots + a + 1).$$

3. Demuestre que el cubo de todo entero puede ser escrito como diferencia de cuadrados. (Sugerencia: note que
$$n^3 = (1^3 + 2^3 + \ldots + n^3) - (1^3 + 2^3 + \ldots + (n-1)^3).$$

4. *a)* Halle los valores de $n \leq 7$ para los cuales $n! + 1$ es un cuadrado perfecto (se desconoce cuándo $n! + 1$ es un cuadrado perfecto para $n > 7$.)
   b) ¿Verdadero o falso? para enteros positivos m y n se cumple $m!n! = (mn)!$ y $m! + n! = (m+n)!$.

5. Demuestre que $n! > n^2$ para todo entero $n \geq 4$, mientras que $n! > n^3$ para todo entero $n \geq 6$.

6. Use la inducción matemática para comprobar la fórmula
$$1(1!) + 2(2!) + \ldots + n(n!) = (n+1)! - 1$$
para todo $n \geq 1$.

1.4. El teorema binomial

En estrecha relación con la notación factorial aparecen los coeficientes binomiales, que se definen para todo par de enteros n, k con $0 \leq k \leq n$ como

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

Al cancelar $k!$ o $(n-k)!$ se obtienen las representaciones equivalentes

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

Por ejemplo,

$$\binom{8}{3} = \frac{8!}{3!5!} = \frac{8\cdot 7\cdot 6\cdot 5\cdot 4}{5!} = \frac{8\cdot 7\cdot 6}{3!} = 56.$$

Observe también que si $k = 0$ o $k = n$, aparece la cantidad $0! = 1$ en la definición del coeficiente binomial, por lo que

$$\binom{n}{1} = \binom{n}{n} = 1.$$

Existe un gran número de identidades relacionadas con los coeficientes binomiales. Entre ellas se destaca la **regla de Pascal**[3].

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k} \qquad (1 \leq k \leq n).$$

Demostración: Al multiplicar la identidad

$$\frac{1}{k} + \frac{1}{n-k+1} = \frac{n+1}{k(n-k+1)}$$

por $\frac{n!}{(k-1)!(n-k)!}$ se obtiene

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

es decir

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

que es la regla de Pascal. **Q.e.d.**

[3]Blaise Pascal (1623-1662)

Esta relación da pie a una configuración conocida como **triángulo de Pascal**, donde el coeficiente binomial aparece como el $k+i$-ésimo número en la n-ésima fila:

$$
\begin{array}{ccccccccccccccccccc}
 & & & & & & & 1 & & & & 1 & & & & & & & \\
 & & & & & & 1 & & & 2 & & & 1 & & & & & & \\
 & & & & & 1 & & & 3 & & & 3 & & & 1 & & & & \\
 & & & & 1 & & & 4 & & & 6 & & & 4 & & & 1 & & \\
 & & & 1 & & & 5 & & & 10 & & & 10 & & & 5 & & & 1 & \\
 & & 1 & & & 6 & & & 15 & & & 20 & & & 15 & & & 6 & & & 1 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
$$

La regla de formación es sencilla. En los bordes del triángulo aparece siempre el número 1 y cualquier número interior es la suma de los dos números más cercanos en la fila inmediata superior.

El llamado **Teorema Binomial** es realmente una regla para desarrollar el binomio $(a+b)^n$ para $n \geq 1$ como suma de potencias de a y b. Esta expresión aparece con mucha frecuencia en la Teoría de Números. Al multiplicar directamente se obtiene

$$
\begin{aligned}
(a+b)^1 &= a+b \\
(a+b)^2 &= a^2+2ab+b^2 \\
(a+b)^3 &= a^3+3a^2b+3ab^2+b^3 \\
(a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4, \text{ etc.}
\end{aligned}
$$

El problema consiste en determinar una fórmula para los coeficientes. Una pista aparece en la comparación con el triángulo de Pascal; se observa que los coeficientes consisten con los números de las correspondientes filas del triángulo de Pascal. Así surge la conjetura

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n,$$

o en forma compacta

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}.$$

La inducción matemática permitirá demostrar la conjetura.

Demostración: Para $n=1$, la fórmula se reduce a

$$(a+b)^1 = \sum_{k=0}^{1}\binom{1}{k}a^k b^{n-k} = \binom{1}{0}a + \binom{1}{1}b = a+b,$$

lo cual es correcto.

Supongamos que la fórmula es cierta para un n fijo y demostremos que se cumple para $n+1$, es decir, que

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

Al desarrollar a partir del miembro izquierdo y aplicar la hipótesis de inducción se tiene

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\ &= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1}.\end{aligned}$$

Pero

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} &= a^{n+1} + \sum_{i=1}^{n}\binom{n}{i-1}a^i b^{n-i+1} \\ \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1} &= \sum_{i=1}^{n}\binom{n}{i}a^i b^{n-i+1} + b^{n+1}.\end{aligned}$$

Entonces

$$(a+b)^{n+1} = a^{n+1} + \sum_{i=1}^{n}\left(\binom{n}{i-1} + \binom{n}{i}\right)a^i b^{n-i+1} + b^{n+1}.$$

Por la regla de Pascal se obtiene finalmente

$$(a+b)^{n+1} = a^{n+1} + \sum_{i=1}^{n}\binom{n+1}{i}a^i b^{n-i+1} + b^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k},$$

como se deseaba demostrar. **Q.e.d.**

La primera formulación aceptable del método de la inducción matemática apareció en el tratado "Traité du Triangle Arithmétique" del matemático y filósofo francés Blaise Pascal en el siglo XVII. Su estudio cuidadoso de las propiedades de los coeficientes binomiales ayudó a sentar las bases de la teoría de las probabilidades.

1.4.1. Ejercicios

1. Para $n \geq 1$ demuestre que

   a) $\binom{n}{k} < \binom{n}{k+1}$ si y sólo si $0 \leq k < \frac{n+1}{2}$.

   b) $\binom{n}{k} = \binom{n}{k+1}$ si y sólo si n es impar y $k = \frac{n+1}{2}$.

2. Para $2 \leq k \leq n-2$ demuestre que

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}, \qquad (n \geq 4).$$

3. Para $n \geq 1$ demuestre las siguientes identidades:

   a) $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$. (Sugerencia: aplique el teorema binomial con con $a = b = 1$.)

   b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \ldots + (-1)^n\binom{n}{n} = 0$

   c) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ldots + n\binom{n}{n} = n2^{n-1}$. (Sugerencia: desarrolle $n(1+b)^{n-1}$ según el teorema binomial y haga $b = 1$, note que $n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$.)

   d) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \ldots + 2^n\binom{n}{n} = 3^n$.

   e) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \ldots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots = 2^{n-1}$. (Sugerencia: Use a) y b).)

4. *a)* Para $n \geq 1$ demuestre que

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \ldots + \binom{n}{2} = \binom{n+1}{3}.$$

   (Sugerencia: use inducción y la regla de Pascal.)

   b) De a) y de $2\binom{m}{2} + m = m^2$ para $m \geq 2$ deduzca la fórmula

$$1^2 + 2^2 + 3^3 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Capítulo 2

EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

2.1. Divisibilidad y números primos

La divisibilidad es una propiedad esencial en el trabajo con los números enteros. Aunque se trata de un tema que puede parecer conocido desde la escuela básica, es importante desarrollarlo con algo de detalle.

Definición 2.1.1

*$t \in \mathbb{Z}$ es un **divisor** de $n \in \mathbb{Z}$ si y sólo si existe $q \in \mathbb{Z}$ tal que $n = tq$. Notación $t|n$.*

PROPIEDADES

1. $1|n$, $n|n$, $n|0$ para todo $n \in \mathbb{N}$.
2. Si $0|n$, entonces $n = 0$.
3. Si $t|n$ y $n|m$, entonces $t|m$.
4. Si $t|n$ y $t|m$, entonces $t|(an + bm)$ para todos $a, b \in \mathbb{Z}$.
5. Si $t|n$, entonces $at|an$ para todo $a \in \mathbb{Z}$.
6. Si $at|an$ y $a \neq 0$, entonces $t|n$.
7. Si $t|n$ y $n \neq 0$, entonces $|t| \leq |n|$.
8. Si $t|d$ y $d|t$, entonces $|t| = |d|$.
9. Si $t|n$ y $d = \frac{n}{t}$, entonces $d|n$.

La demostración de estas propiedades es sencilla y queda como ejercicio al lector.

El algoritmo de la división juega un papel esencial en relación con la divisibilidad.

TEOREMA 2.1.1 ***Algoritmo de la división***

Si a, b son números enteros ($b \neq 0$), entonces existen números enteros únicos q, r tales que $a = bq + r$, siendo $0 \leq r < b$.

Demostración:

(Existencia:) Sea $S = \{a - bk \geq 0; k \in \mathbb{Z}\}$. Entonces es $S \neq \emptyset$, pues $a - bk \geq 0$ si $k \leq \frac{a}{b}$. Además es $S \subset \mathbb{Z}_+$. De todo ello se deduce que existe un menor elemento en S, al que denotamos por r. Es obvio que $r \geq 0$.

Si fuera $r \geq b$, entonces $r - b \geq 0$. Pero $r - b = a - bq - b = a - b(q + 1) \geq 0$ y $a - b(q + 1) < a - bq$, de donde se tiene que $0 \leq r - b < a - bq$, o sea, $r - b$ es un elemento de S menor que $a - bq$, lo cual constituye una contradicción.

Entonces es $a = bq + r$, con $0 \leq r < b$.

(Unicidad:) Sea $a = bq_1 + r_1 = bq_2 + r_2$, con $0 \leq r_1, r_2 < b$. Entonces se cumple que $b(q_1 - q_2) = r_2 - r_1$, o sea $b|(r_2 - r_1)$. Pero $-b < r_2 - r_1 < b$, luego es $r_2 - r_1 = 0$, de donde $q_1 - q_2 = 0$. **Q.e.d**

NOTA: ± 1 y $\pm n$ son **divisores triviales** de n.

MÁXIMO COMÚN DIVISOR Y MÍNIMO COMÚN MÚLTIPLO

Otros actores destacados de la Teoría de Números son el máximo común divisor y el mínimo común múltiplo que se presentan en este epígrafe.

DEFINICIÓN 2.1.2

*Dados los números naturales (no todos nulos) $a_1, \ldots, a_n$, existe un único número natural d, llamado **máximo común divisor de** $a_1, \ldots, a_n$, tal que*

1. *$d|a_k$ para $k = 1, \ldots, n$;*
2. *si $t|a_k$ para $k = 1, \ldots, n$, entonces $t|d$.*

Notación: $d = mcd(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$.

Demostración de la existencia y unicidad de d:

Sea D el conjunto de todos los divisores comunes positivos de los a_k para los índices $k = 1, \ldots, n$. Es claro que $1 \in D$, por lo que $D \neq \emptyset$. D es un conjunto finito de números enteros positivos, por lo que tiene un mayor elemento d, que es el máximo común divisor buscado. **Q.e.d.**

NOTA: Resulta sencillo comprobar que (demostración de ejercicio)

- Si $d = (m, n)$, existen n_1 y m_1 tales que $n = dn_1$, $m = dm_1$ y $(m_1, n_1) = 1$.
- $(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$.

Definición 2.1.3

Dados los números naturales (no todos nulos) $a_1, \ldots, a_n$. Existe un único número natural v, llamado ***mínimo común múltiplo de*** *$a_1, \ldots, a_n$, tal que*

1. *$a_k | v$ para $k = 1, \ldots, n$;*
2. *si $a_k | w$ para $k = 1, \ldots, n$, entonces $v | w$.*

Notación: $v = mcm(a_1, \ldots, a_n) = [a_1, \ldots, a_n]$.

La demostración de la existencia y unicidad de v es análoga a la anterior y queda como ejercicio.

RELACIÓN ENTRE MCD Y MCM

$$(a, b)[a, b] = ab.$$

La demostración de esta propiedad queda como ejercicio.

El máximo común divisor puede ser hallado, por supuesto, listando todos los posibles divisores y seleccionando el mayor, pero para números grandes ese procedimiento es muy trabajoso. En el libro VII de "Elementos" se propone una técnica mejor basada en la aplicación repetida del algoritmo de la división. A pesar de que existe evidencia histórica de que dicho procedimiento es anterior a Euclides, el mismo es conocido actualmente como el algoritmo de Euclides.

Lema 2.1.1

Sean c, d enteros tales que $c = dq + r$. Entonces es $(c, d) = (d, r)$.

Demostración: Si $e|c$, $e|d$ y $c = dq + r$, entonces $e|r$, por lo que e es divisor común de d y r. Análogamente, si $e|d$, $e|r$ y $c = dq + r$, entonces $e|c$, de donde e es divisor común de c y d. Luego, los divisores comunes de c, d y de d, r coinciden, por lo que $(c, d) = (d, r)$. **Q.e.d.**

Sea ahora $a \geq b$. Buscamos (a, b). Para ello sea $a = r_0, b = r_1$. Entonces por el algoritmo de la división es

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \quad \text{con} \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3 \quad \text{con} \quad 0 \leq r_3 < r_2 \\ \ldots &\quad \ldots \quad \ldots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \quad \text{con} \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_n q_n \end{aligned}$$

Nótese que siguiendo los pasos anteriores se obtiene una sucesión

$$r_0 > r_1 > \ldots > r_n \geq 0,$$

lo cual justifica que se alcance en algún momento el resto cero. Por el Lema 2.1.1 es entonces

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Este análisis constituye de por sí la demostración del teorema siguiente .

TEOREMA 2.1.2 ***El algoritmo de Euclides***

Sean $a \geq b > 0$, $a = r_0$, $b = r_1$. Aplicando sucesivamente el algoritmo de la división se obtiene

$$\begin{aligned} r_k &= r_{k+1} q_{k+1} + r_{k+2} \quad \textit{con} \quad 0 \leq r_{k+2} < r_{k+1} \quad \textit{para} \quad k = 0, 1, \ldots, n \\ r_{n+1} &= 0. \end{aligned}$$

Entonces es $(a, b) = r_n$.

EJEMPLO:

$$\begin{aligned} 252 &= 1(198) + 54 \\ 198 &= 3(54) + 36 \\ 54 &= 1(36) + 18 \\ 36 &= 2(18). \end{aligned}$$

Entonces es $(252, 198) = 18$.

También se puede utilizar el algoritmo de la división de Euclides para escribir (a, b) como combinación lineal de a y b. Para ello, despejando las igualdades anteriores en sentido inverso se tiene

$$18 = 54 - 36 = 54 - (198 - 3(54)) = 4(54) - 198 = 4(254 - 198) - 198,$$

de donde $18 = 4(254) - 5(198)$.

Este resultado se expresa en el teorema siguiente:

TEOREMA 2.1.3 *Si $d = (a, b)$, entonces existen $x, y \in \mathbb{Z}$ tales que*

$$d = ax + by.$$

Resulta obvio que la aplicación de este algoritmo para determinar el máximo común divisor de dos números puede resultar extensa. En cuanto al número de paso necesarios se conoce (entre otros) el siguiente resultado, que se debe a Lamé[1] y ofrecemos sin demostración.

TEOREMA 2.1.4 ***Teorema de Lamé***

El número de pasos del algoritmo de la división de Euclides para determinar el máximo común divisor de dos enteros no excede al quíntuplo del número de dígitos del menor entero.

En el caso de trabajar con más de dos números se tiene el siguiente resultado:

TEOREMA 2.1.5 *Si $d = (c_1, \ldots, c_n)$, entonces existen $x_1, \ldots, x_n \in \mathbb{Z}$ tales que*

$$d = c_1x_1 + \ldots + c_nx_n.$$

Demostración: (Inducción)

- Sea $n = 2$ y $c_1 > c_2$ no nulos. Haciendo $c_1 = a_0$ y $c_2 = a_1$ y recorriendo el algoritmo de Euclides de arriba hacia abajo se obtiene

$$\begin{array}{rcl} a_2 & = & a_0 - a_1q_1 = a_0\xi_2 - a_1\eta_2 \\ \ldots & \ldots & \ldots \\ a_n & = & a_{n-2} - a_{n-1}q_{n-1} = a_0\xi_n - a_1\eta_n, \end{array}$$

  con $\chi_n, \eta_n \in \mathbb{Z}$. Haciendo $\xi_n = x_1, \eta_n = x_2$ se tiene

$$d = c_1x_1 + c_2x_2.$$

- Sea válido el teorema para n.
- Para $n + 1$ se tiene

$$\begin{array}{rcl} (c_1, \ldots, c_{n+1}) & = & ((c_1, \ldots, c_n), c_{n+1} \\ & = & (c_1, \ldots, c_n)x + c_{n+1}x_{n+1} \\ & = & (c_1x_1 + \ldots + c_nx_n)x + c_{n+1}x_{n+1}, \end{array}$$

  lo que demuestra el teorema. **Q.e.d.**

[1] Gabriel Lamé (1795-1870)

El siguiente teorema resulta una importante consecuencia del algoritmo de Euclides.

TEOREMA 2.1.6 *Si $k > 0$, entonces $(ka, kb) = k(a, b)$.*

Demostración: Al multiplicar cada una de las ecuaciones del algoritmo de Euclides por k se obtiene

$$\begin{array}{rcll} ak & = & q_1(bk) + r_1k & \text{con} \quad 0 \leq r_1 < b \\ b & = & q_2(r_1k) + r_2k & \text{con} \quad 0 \leq r_2 < r_1 \\ r_1 & = & q_3(r_2k) + r_3k & \text{con} \quad 0 \leq r_3 < r_2 \\ \cdots & \cdots & \cdots \quad \cdots & \\ r_{n-2} & = & q_n(r_{n-1}k) + r_nk & \text{con} \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & q_{n+1}(r_nk) + 0. & \end{array}$$

Pero esto es obviamente el algoritmo de Euclides aplicado a los números ka y kb, de modo que $(ka, kb) = r_nk = k(a, b)$. **Q.e.d.**

COROLARIO 2.1.1 *Para todo entero $k \neq 0$ se cumple $(ka, kb) = |k|(a, b)$.*

Demostración: Basta considerar el caso $k < 0$, donde $-k = |k| > 0$. Aplicando el teorema anterior es

$$(ka, kb) = (-ka, -kb) = (|k|a, |k|b) = |k|(a, b).$$

Q.e.d.

Una demostración alternativa del teorema 2.1.6 funciona como sigue: (ak, bk) es el menor entero positivo de la forma $(ak)x + (bk)y$, por lo que es k veces el menor entero de la forma $ax + by$. Este último valor es $k(a, b)$. **Q.e.d.**

Para ilustrar el teorema 2.1.6 observe que

$$(12, 30) = 3(4, 10) = 3 \cdot 2(2, 5) = 6 \cdot 1 = 6.$$

NÚMEROS PRIMOS

Si importante es todo lo presentado hasta ahora, el concepto de número primo puede ser considerado el más importante de toda la Teoría de Números. Es que no solo se trata del concepto que da pie al Teorema Fundamental de la Aritmética, sino que sin ellos no existiría la criptografía actual que garantiza la seguridad de las comunicaciones.

DEFINICIÓN 2.1.4

*Un número entero $p > 1$ se dice **primo** si sólo tiene divisores triviales. Un número que no es primo se dice **compuesto**.*

TEOREMA 2.1.7 *Todo número natural $n > 1$ tiene al menos un divisor primo. El menor divisor primo de n no es mayor que $\sqrt{n}$.*

Demostración: Sea $A = \{a \in \mathbb{N};\ a > 1,\ a|n\}$. $A \neq \emptyset$, pues $n \in A$. Entonces A tiene un menor elemento p. Si p no fuera un número primo, entonces existe $q > 1$ que divide a p, por lo que $q|a$ y $q < p$, lo que contradice la selección de p.

Sea q el menor divisor primo de n. Entonces existe un entero $n_1 \geq q$ tal que $n = qn_1$. Multiplicando por q la desigualdad $n_1 \geq q$, se tiene que $n = qn_1 \geq q^2$, de donde se deduce que $q < \sqrt{n}$. **Q.e.d.**

Llegados a este punto surge una pregunta natural ¿existe un mayor número primo o la lista continua indefinidamente? La respuesta aparece en una demostración notablemente sencilla dada por Euclides en el Libro IX de "Elementos". El argumento de Euclides es reconocido universalmente como modelo de elegancia matemática. La idea es la siguiente: dada cualquier lista finita de números primos, siempre se puede encontrar un número primo que no pertenece a la lista, por lo que hay infinitos números

TEOREMA 2.1.8 *Existen infinitos números primos.*

Demostración: (Euclides) Supongamos que existe sólo una cantidad finita de números primos

$$p_1 = 2,\ p_2 = 3, \ldots,\ p_n.$$

Sea el número

$$p = p_1 p_2 \cdots p_n + 1.$$

Por el teorema 2.1.7 existe un número primo q tal que $q|p$. Si fuera $q = p_i$ para algún $i = 1, \ldots, n$, de la relación anterior se tendría que $q|1$, lo cual no es posible. Entonces p es un nuevo número primo. **Q.e.d.**

A continuación se presenta un famoso método, conocido como **Criba de Eratóstenes**[2], para determinar todos los números primos no mayores que un número n.

1. Se escriben todos los números enteros no mayores que n
2. Se tacha el número 1.
3. El próximo número no tachado es el 2. Se comprueba si 2 es menor o igual a $\sqrt{n}$ y en caso positivo se circula y se tachan todos sus múltiplos.

[2]Erathostenes (276-196 A.C.)

4. Se continua repitiendo el procedimiento hasta que no queden números sin marcar.

5. Los números circulados son todos los números primos que no exceden al número dado n.

EJEMPLO: La siguiente tabla muestra el procedimiento de la Criba de Eratóstenes aplicado a $n = 100$.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Así, los números primos menores que 100 son $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Uno de los temas que más han interesado a los matemáticos y uno de los más indescifrables se refiere a la distribución de los números primos, pero esto sigue siendo un misterio. Repetidamente se pueden encontrar ciertos patrones en su distribución, pero aún no se encuentra un modelo preciso. La diferencia entre primos consecutivos puede ser pequeña como en los pares 11 y 13, 17 y 19, o 1 000 000 000 061 y 1 000 000 000 063. Pero también se pueden encontrar intervalos arbitrariamente largos de enteros totalmente desprovistos de cualquier número primo. Resulta fácil comprobar que dado un número entero n, los números $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$ son todos compuestos, dado que k divide a $(n+1)! + k$, siendo $k = 1, ..., n+1$. De ello se deduce el siguiente teorema.

TEOREMA 2.1.9

Para todo valor entero positivo de n, existen n números compuestos consecutivos.

Una pregunta natural es la relativa a encontrar una cota del n-ésimo número primo. El siguiente teorema presenta una cota bien elemental, que se deduce a partir de la infinitud de los números primos.

TEOREMA 2.1.10 *Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.*

Demostración: (por inducción en n).

(1) Obviamente se cumple la acotación para $n = 1$.

(2) Como hipótesis de inducción se asume que la acotación se cumple para todo entero menor o igual que n.

(3) Entonces

$$\begin{aligned} p_{n+1} &\leq p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\ldots+2^{n-1}} + 1. \end{aligned}$$

Aplicando la identidad $1 + 2 + 2^2 + \ldots + 2^{n-1} = 2^n - 1$, se obtiene

$$p_{n+1} \leq 2^{2^n-1} + 1.$$

Pero $1 \leq 2^{2^n-1}$, de donde

$$p_{n+1} \leq 2^{2^n-1} + 2^{2^n-1} = 2 \cdot 2^{2^n-1} = 2^{2^n},$$

lo que completa la demostración. **Q.e.d.**

De aplicar directamente el teorema anterior a $p_1, \ldots, p_{n+1}$ se deduce que para $n \geq 1$ existen al menos $n + 1$ primos menores que 2^{2^n}.

Existen numerosos problemas interesantes referidos a los números primos y muchos de ellos aún no han sido resueltos. A continuación se presentan algunos de ellos.

PRIMOS GEMELOS

Hoy permanece abierta la pregunta sobre si hay infinitos pares de primos gemelos, es decir, pares de primos impares sucesivos $(p, p + 2)$. La evidencia numérica conduce a sospechar una conclusión afirmativa. Sin embargo, las computadoras han descubierto 152 892 pares de primos gemelos menores que 30 000 000 y veinte pares entre 10^{12} y $10^{12} + 10000$, lo que podría sugerir su creciente escasez al aumentar en magnitud los enteros positivos. Por otra parte, solo existe una terna de primos trillizos $(p, p + 2, p + 4)$ ¿se anima a encontrarla?

LA CONJETURA DE GOLDBACH

Otro problema famoso se conoce como la conjetura de Goldbach. En una carta a Euler[3] (1742), Christian Goldbach[4] formuló una hipótesis de la que se podía deducir que cada entero par es la suma de dos números primos o 1. Una formulación algo más general es que cada entero par mayor o igual que 4 puede escribirse como una suma de dos números primos. Esto es fácil de confirmar para los primeros enteros pares:

$$\begin{aligned} 4 &= 2+2 \\ 6 &= 3+3 \\ 8 &= 3+5 \\ 10 &= 3+7 \\ 12 &= 5+7\ldots \end{aligned}$$

Parece ser que Euler nunca trató de probar el resultado, pero en respuesta a Goldbach presentó una nueva conjetura: todo entero par ($k \geq 6$) de la forma $k = 4n + 2$ es suma de dos números primos de la forma $4n + 1$ o 1.

De la validez de la conjetura de Goldbach se deduce otra más débil que plantea que todo número impar a partir de 7 se puede expresar como suma de tres números primos.

La evidencia numérica de la veracidad de esas conjeturas es agobiante. La mayor aproximación a su comprobación es el resultado del matemático Chen[5], que demostró que todos los enteros pares mayores que cierto número (grande) C son suma de dos primos. Pero C es un número muy grande y, a pesar de o que se ha logrado adelantar gracias a la computación, aún no se logra cerrar la brecha. Decía Landau[6] que

> "*La conjetura de Goldbach es falsa para a lo sumo* 0 % *de los enteros; ese a lo sumo* 0 % *no excluye, por supuesto, la posibilidad de que existan infinitas excepciones.*"

Nótese que si la conjetura es cierta, entonces todo número impar mayor que 7 tiene que ser la suma de tres primos. Pues si n es un entero impar mayor que 7, entonces $n - 3$ es par mayor que 4 es por tanto, suma de dos primos, por lo que n será suma de tres primos. En 1937 Vinogradov[7] demostró que ello es válido para todo entero impar suficientemente grande, es decir, mayor que cierto N (N es un número de 6 846 180 cifras). Nuevamente queda en "manos" de las computadoras la tarea de

[3]Leonhard Euler (1707-1783)
[4]Christian Goldbach (1690-1764)
[5]Chen Jingrun (1933-1996)
[6]Lev Landau (1908-1968)
[7]Ivan Vinogradov (1891-1983)

llenar la brecha. Hasta el año 2008 se había logrado demostrar computacionalmente la conjetura para todo $n \leq 12 \cdot 10^{17}$. Ello significa que aún restaban por calcular unos $3\dot{1}0^{17}(1,11 \cdot 10^{42981} - 4)$ números, es decir, la cantidad de números que faltan por calcular es de más de 43000 cifras. Pero,... esta parte de la historia encontró un final feliz cuando en el año 2015 el matemático peruano Harald Helfgott[8] logró finalmente demostrar la conjetura débil de Goldbach.

SUCESIONES DE NÚMEROS PRIMOS

Nótese ahora que cada entero positivo puede escribirse en una de las formas

$$4n, 4n+1, 4n+2, 4n+3.$$

Entonces los enteros impares entran en dos progresiones: una que contiene a los enteros de la forma $4n+1$,

$$1, 5, 9, 13, 17, 21, \ldots$$

y la otra que contiene a los enteros de la forma $4n+3$,

$$3, 7, 11, 15, 19, 23, \ldots$$

Mientras que cada una de esas progresiones incluye obviamente algunos números primos, la pregunta es cuál de ellas contiene infinitos primos. Esto brinda la oportunidad de desarrollar el método de Euclides para demostrar la infinitud de los primos. Una ligera modificación del argumento revela que hay un número infinito de primos de la forma $4n+3$, partiendo del conocimiento (de fácil demostración) de que el producto de enteros de la forma $4n+1$ es de la misma forma.

TEOREMA 2.1.11 *Existen infinitos primos de la forma $4n+3$.*

Demostración: Supongamos que existen solo finitos primos de la forma $4n+3$, que denotamos por $q_1, q_2, \ldots, q_s$. Consideremos el entero positivo

$$N = 4q_1q_2 \cdots q_s - 1 = 4(q_1q_2 \cdots q_s - 1) + 3$$

y sea $N = r_1r_2...r_t$ su factorización prima. Como N es impar, se tiene que $r_k \neq 2$ para todo k, por lo que todo r_k es de la forma $4n+1$ ó $4n+3$. Entonces, para que N tenga la forma $4n+3$ tiene que contener al menos un factor primo r_i de esa forma. Pero ese r_i no puede aparecer en la lista $q_1, q_2, \ldots, q_s$, pues llevaría a la contradicción de que $r_i|1$. La única conclusión posible es que existen infinitos primos de la forma $4n+3$. **Q.e.d.**

Una pregunta razonable ahora se refiere a si es también infinito el número de primos de la forma $4n+1$. La respuesta es afirmativa, pero la demostración debe esperar por el desarrollo de las herramientas matemáticas necesarias. Ambos resultados son casos particulares de un famoso teorema de Dirichlet[9] sobre primos en progresión

[8] Harald Helfgott (1977-)
[9] Peter Gustav Dirichlet (1805-1859)

aritmética demostrado en 1837, que se presenta a continuación sin demostración.

TEOREMA 2.1.12 ***Dirichlet***

Si a y b son enteros positivos primos relativos, entonces la progresión aritmética

$$a + b, a + 2b, a + 3b, \ldots$$

contiene infinitos primos.

No existe progresión aritmética $a + b, a + 2b, a + 3b, \ldots$ que consista sólo de números primos. Para comprobarlo, suponga que $a + nb = p$, siendo p primo. Si hacemos $n_k = n + kp$ para $k. = 1, 2, 3, \ldots$, entonces el término n_k-ésimo de la progresión es

$$a + n_k b = a + (n + kp)b = (a + nb) + kpb = p + kpb.$$

Como ambos términos del miembro derecho son divisibles por p, también lo es $a+n_k b$. En otras palabras, la progresión contiene infinitos números compuestos.

Se ha conjeturado que existen progresiones aritméticas de longitud finita arbitraria compuestas de primos consecutivos. Ejemplos de esas progresiones con 3 y 4 primos respectivamente son $41, 47, 53$ y $251, 257, 263, 269$. No hace mucho tiempo, una búsqueda computacional reveló progresiones de 5 y 6 primos consecutivos, cuyos términos tienen la diferencia común 30, ellas comienzan con los primos 9 843 019 y 121 174 811. No se ha podido encontrar hasta el momento una progresión aritmética consistente en 7 primos consecutivos. Si se elimina la restricción de que los números primos sean consecutivos, entonces es posible encontrar infinitos conjuntos de 7 primos en progresión aritmética, como $7, 157, 307, 457, 607, 757, 907$.

FÓRMULAS GENERADORAS DE NÚMEROS PRIMOS

Aquí va otro famoso problema que hasta ahora se ha resistido el ataque más determinado. Durante siglos los matemáticos han buscado una fórmula que produzca todos los números primos o, en su defecto, una fórmula que sólo produzca números primos. El problema parece sencillo: encontrar una función $f(n)$ con dominio en los enteros no negativos y cuya imagen sea cierto subconjunto infinito del conjunto de todos los números primos. En la Edad Media se creía que el polinomio cuadrático

$$f(n) = n^2 + n + 41$$

producía sólo números primos. Se puede comprobar que la afirmación es correcta para $n = 0, 1, \ldots, 39$. Pero la conjetura falla en los casos $n = 40$ y $n = 41$, donde aparece el factor 41

$$f(40) = 40^2 + 40 + 41 = 41^2 \quad \text{y} \quad f(41) = 41^2 + 41 + 41 = 41 \cdot 43.$$

El siguiente factor $f(42) = 1747$ retorna a ser primo. No se conoce aún si la fórmula $f(n) = n^2 + n + 41$ produce infinitos valores primos para enteros n.

La falla de la función anterior en la producción de primos no es accidental, es fácil comprobar que no existe polinomio no constante $f(n)$ con coeficientes enteros que tome sólamente valores primos para enteros n. Supongamos que existe dicho polinomio

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + \ldots + a_2 n^2 + a_1 n + a_0,$$

donde todos los coeficientes $a_0, \ldots, a_k$ son enteros y $a_k \neq 0$. Para un valor fijo $n = n_0$, sea $p = f(n_0)$ un número primo. Ahora para cualquier entero t consideramos la expresión $f(n_0 + tp)$:

$$\begin{aligned} f(n_0 + tp) &= a_k(n_0 + tp)^k + \ldots + a_1(n_0 + tp) + a_0 \\ &= a_k n_0^k + \ldots + a_1 n_0 + a_0 + pQ(t) \\ &= f(n_0) + pQ(t) \\ &= p + pQ(t) = p(1 + Q(t)), \end{aligned}$$

donde $Q(t)$ es un polinomio en t con coeficientes enteros. De aquí que $p | f(n_0 + tp)$, y como $f(n)$ sólo toma valores primos, tiene que ser $f(n_0 + tp) = p$ para todo entero t. Pero esto contradice el hecho de que un polinomio de grado k no puede asumir el mismo valor más de k veces.

También han existido éxitos en la búsqueda de funciones productoras de primos. W. H. Mills demostró (1947) que existe un número real positivo r tal que la expresión $f(n) = \left[r^{e^n}\right]$ es primo para $n = 1, 2, 3, \ldots$ (los corchetes denotan la función parte entera). Claro que se trata sólo de un teorema de existencia y nada se sabe sobre el valor real de r.

CANTIDAD DE PRIMOS MENORES QUE UN ENTERO DADO

La gran pregunta es ¿cuántos números primos menores que n existen ?

La respuesta a esta pregunta no es sencilla, ni es posible darla con exactitud. Aunque la sucesión de los números primos presenta grandes irregularidades, el Teorema de los Números Primos permite predecir, para grandes números, cuántos hay por debajo de un entero dado. Pero el resultado no es exacto, sino en "en promedio" o en "sentido probabilístico". El siguiente teorema, que se presentará más adelante, ofrece una estimación.

Teorema 2.1.13

Si $\pi(x)$ representa la cantidad de números primos menores que x, entonces se cumple

$$\pi(x) = \int_0^x \frac{\mathrm{d}t}{\ln t},$$

de donde se deduce

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

2.1.1. Ejercicios

1. Encuentre q y r en el algoritmo de la división con divisor 17 y dividendo
   a) 100 b) -44
2. ¿Qué puede concluir si a, b son enteros no nulos tales $a|b$ y $b|a$?
3. Demuestre que
   a) Si $a, b, c, d \in \mathbb{Z}$, $a \neq 0, c \neq 0$, tal que $a|b$ y $c|d$, entonces $ac|bd$.
   b) Si $a, b, c \in \mathbb{Z}$, $c \neq 0$, entonces $a|b$ si y sólo si $ac|bc$.
   c) Si $a, b, c \in \mathbb{Z}$ tal que $a|bc$ y a es un número positivo solo divisible por 1 y por a, entonces $a|b$ o $a|c$.
   d) Si $a, b \in \mathbb{Z}$ tal que $a|b$, entonces $a^k|b^k$.
4. Demuestre que si x es un número real positivo, entonces el número de enteros menores o iguales a x que son divisibles por un numero entero positivo d es igual a $\left[\frac{x}{d}\right]$.
5. Encuentre el número de enteros positivos que no excedan de 1000 y que no sean divisibles por $3, 5$ ó 7.
6. a) Demuestre que el producto de 3 enteros consecutivos es divisible por 6.
   b) Utilice la inducción matemática para demostrar que $n^5 - n$ es divisible por 5 para todo valor entero positivo de n.
7. Halle:
   a) $(15, 35)$ c) $(-27, 45)$ e) $(11, 121)$
   b) $(0, 111)$ d) $(90, -100)$ f) $(1001, 289)$
8. Sea a un número entero positivo. Halle:
   a) $(a, 2a)$ b) $(a, a+1)$ c) $(a, a+2)$

9. Demuestre que si $a, b, c \in \mathbb{Z}$, entonces es $(ca, cb) = |c|(a, b)$.

10. Demuestre que si $(a, b) = 1$, entonces es $(a + b, a - b) = 1$ ó 2.

11. Halle $(a^2 + b^2, a + b)$ ¿Qué sucede si $(a, b) = 1$?

12. a) Demuestre que

$$(a,b) = \begin{cases} 2(\frac{a}{2}, \frac{b}{2}) & \text{si } a, b \text{ son pares.} \\ (\frac{a}{2}, b) & \text{si } a \text{ par, } b \text{ impar} \\ (a-b, b) & \text{si } a, b \text{ impares con } a > b \\ a & \text{si } a = b \end{cases}$$

    b) Calcule mediante este algoritmo $(2106, 8318)$.

    c) Elabore un programa que determine el máximo común divisor entre dos números a través de este algoritmo.

13. Demuestre que $(a, b)[a, b] = ab$.

14. Demuestre que $(3m + 2, 5m + 3) = 1$ para todo entero positivo m.

15. Halle un trío de enteros mutuamente primos tal que dos de ellos no sean primos relativos.

16. Halle cuatro enteros mutuamente primos tal que tres de ellos no lo sean.

17. Halle:
    a) $(45, 75)$ c) $(666, 1414)$
    b) $(102, 222)$ d) $(20785, 44350)$

18. Exprese los resultados del ejercicio anterior como combinación lineal.

19. Encuentre todos los números primos que son diferencias de cuartas potencias de dos enteros.

20. Demuestre que si el menor factor primo p de un número entero positivo n es mayor que $\sqrt[3]{n}$, entonces $\frac{n}{p}$ es primo ó 1.

21. Demuestre que para $p > 3$ no existen triplos primos $(p, p + 2, p + 4)$.

22. Use el segundo principio de inducción matemática para demostrar que todo número entero positivo n mayor que 1 es primo o producto de dos o mas primos.

2.2. El Teorema Fundamental de la Aritmética

El Teorema Fundamental de la Aritmética es uno de los más demostrados. Se habla de un número realmente grande de demostraciones, por ejemplo, Gauss es autor de más de cinco demostraciones diferentes. A continuación se presentan dos lemas que ayudan a su comprensión.

LEMA 2.2.1

Sean a, b, c enteros positivos tales que $(a, b) = 1$ y $a|bc$. Entonces $a|c$.

Demostración: Si $(a, b) = 1$, existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$. Entonces $c = (ax + by)c = a(cx) + bc(y)$. Pero $a|a$ y $a|bc$, de donde $a|c$. **Q.e.d.**

LEMA 2.2.2

Sea p un número primo tal que $p|a_1a_2a_3 \dots a_n$ con $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Entonces existe un entero positivo i tal que $p|a_i$.

Demostración: (Por inducción)

i) Sea $n = 1$. Entonces $p|a_1$.

ii) Sea cierto el lema para un valor entero de n.

iii) Sea $p|a_1a_2a_3 \dots a_na_{n+1}$. Como p es primo, entonces

$$p|a_1a_2a_3 \dots a_n \quad \text{ó bien} \quad p|a_{n+1}.$$

Ahora si $p|a_{n+1}$, entonces es $i = n + 1$.

Por otra parte, si $p|a_1a_2a_3 \dots a_n$, entonces la hipótesis de inducción ii) garantiza la validez del lema. **Q.e.d.**

TEOREMA 2.2.1 ***Teorema Fundamental de la Aritmética***

Todo número natural $n > 1$ se puede representar de modo único (excepto quizás por el orden) como producto de números primos.

Demostración:

(Existencia): Si $n > 1$, por el teorema 2.1.7 existe un número primo p_1 tal que $n = p_1n_1$. Si $n_1 = 1$ se tiene la representación buscada. Si $n_1 \neq 1$, nuevamente por el teorema 2.1.7 existe un número primo p_2 tal que $n_1 = p_2n_2$, de modo que $n = p_1p_2n_2$. De ese modo se repite el proceso hasta obtener

$$n = p_1p_2 \cdots p_rn_r$$

con $n_r = 1$. Es decir,

$$n = p_1 p_2 \cdots p_r.$$

(Unicidad): Sean

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

dos representaciones de n como producto de números primos. Como

$$p_i | q_1 q_2 \cdots q_s$$

para todo $i = 1, \ldots, r$ y q_k es primo para todo $k = 1, \ldots, s$, entonces es $p_i = q_k$ para algún k. Reordenando los q_k (sin perder generalidad), se tiene que $p_i = q_i$ para todo $i = 1, \ldots, r$, de donde $r \leq s$. Repitiendo este análisis (ahora partiendo de la representación a la derecha) se obtiene que $s \leq r$, lo que implica la unicidad de la representación. **Q.e.d.**

Este teorema justifica la existencia de lo que se conocce como representación canónica de un número natural.

REPRESENTACIÓN CANÓNICA

$$\begin{aligned} n &= \prod_{i=1}^{k} p_i^{\alpha_i}, \qquad p_1 < p_2 < \ldots < p_k, \quad \alpha_i \geq 1 \\ &= \prod_{p \in P} p^{\alpha_p}, \qquad \alpha_p > 0 \text{ sólo para finitos primos } p. \end{aligned}$$

EJEMPLO: Hallar todos los divisores positivos de 120.

Al descomponer 120 en factores primos es $120 = (2^3)(3)(5)$.

1	3	5	$3 \cdot 5$
2	$(2)(3) = 6$	$(2)(5) = 10$	$(2)(3)(5) = 30$
$2^2 = 4$	$(2^2)(3) = 12$	$(2^2)(5) = 20$	$(2^2)(3)(5) = 60$
$2^3 = 8$	$(2^3)(3) = 24$	$(2^3)(5) = 40$	$(2^3)(3)(5) = 120$

Entonces todos los divisores positivos de 120 son $1, 2, 3,\ 4, 5, 6, 8, 10,\ 12, 15,\ 20,\ 24, 30, 40, 60, 120$.

NOTA: Este teorema **no es válido** en otros dominios numéricos, por ejemplo, sea

$$\mathbb{M} = \{m \in \mathbb{N};\ m = 4n + 1,\ n \in \mathbb{N} \cup \{0\}\}.$$

Si se define en este dominio número primo en la forma usual, los primeros números primos son $5, 9, 13, 17, 21, 29, 33, \ldots$. En este caso se tiene que

$$693 = 4 \cdot 173 + 1 \in \mathbb{M} \qquad \text{y} \qquad 693 = 9 \cdot 77 = 21 \cdot 33.$$

El siguiente resultado es de gran utilidad para determinar la irracionalidad de ciertos números.

TEOREMA 2.2.2

Sea α raíz de $x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ con $c_k \in \mathbb{Z}$ para todo $0 \leq k \leq n$ entero, entonces α es entero o irracional.

Demostración: Supongamos que α es racional, es decir $\alpha = \frac{a}{b}$ con $(a, b) = \pm 1$. Entonces

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \ldots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Al multiplicar por b^n es

$$a^n + c_{n-1}a^{n-1}b + \ldots + c_1 ab^{n-1} + c_0 b^n = 0,$$

de donde

$$a^n = b(-c_{n-1}a^{n-1} - \ldots - c_1 ab^{n-2} - c_0 b^{n-1})$$

De aquí que $b|a^n$.

Si fuera $b = \pm 1$, entonces es $\alpha \in \mathbb{Z}$. En cambio, si $b \neq \pm 1$, entonces b tiene divisor primo p. Es decir, $p|b$, por lo que $p|a^n$, de donde $p|a$. De aquí que a y b tienen un divisor común primo p, lo cual es imposible, pues $(a, b) = 1$. Entonces $\alpha \notin \mathbb{Q}$. **Q.e.d.**

EJEMPLO: Sea $a > 0$. Entonces $x^n - a = 0$ implica que $x^n = a$, es decir, $x = \sqrt[n]{a}$. Entonces $\sqrt[n]{a} \in \mathbb{Z}$ ó $\sqrt[n]{a} \notin \mathbb{Q}$. De aquí se deduce que $\sqrt{2}$, $\sqrt[3]{2}$, etc. son irracionales.

El Teorema Fundamental de la Aritmética garantiza que todo número entero mayor que 1 se puede factorizar de modo único en factores primos. Sin embargo, dicha factorización puede resultar en extremo laboriosa, pues, por ejemplo, para factorizar $11687 = 13 \cdot 29 \cdot 31$, se debe probar la divisibilidad de dicho número por $3, 5, 7, 11$ antes de encontrar el primer factor 13.

El único criterio que permite aligerar el trabajo es que se conoce que si n no es primo, entonces tiene al menos un factor primo menor o igual que $\sqrt{n}$ (¡pero $\sqrt{n}$ puede ser enorme!).

El criterio siguiente que puede ser más eficiente en ciertos casos.

LEMA 2.2.3

Sea n positivo impar. Entonces existe una correspondencia uno a uno entre las factorizaciones de n en dos enteros positivos y las representaciones de n como diferencia de cuadrados.

Demostración: Si $n = ab$, entonces es

$$n = s^2 - t^2 \quad \text{con} \quad s = \frac{a+b}{2}, t = \frac{a-b}{2}$$

Recíprocamente, si $n = s^2 - t^2$, entonces es

$$n = ab \quad \text{con} \quad a = (s-t), b = (s+t).$$

Q.e.d.

LA FACTORIZACIÓN DE FERMAT

En un fragmento de una cart, escrita con gran probabilidad al Padre Marin Mersenne[10] en 1643, Fermat[11] describe una técnica para factorizar números grandes. Este representa el primer intento real sobre el método clásico de tratar de encontrar un factor de n dividiendo por todos los primos que no exceden a $\sqrt{n}$. El esquema de la factorización de Fermat tiene como esencia la observación de que la búsqueda de factores de un entero impar n (como los múltiplos de 2 son fácilmente reconocibles, no se pierde generalidad al asumir que n es impar) es equivalente a encontrar soluciones enteras x, y de la ecuación

$$n = s^2 - t^2.$$

Para solucionar la ecuación $n = s^2 - t^2$. Las soluciones se obtienen de $t^2 - n$, $(t+1)^2 - n$, $(t+2)^2 - n$, ..., con $t = [\sqrt{n}] + 1$. El método termina en algún momento, pues $n = (\frac{n+1}{2})^2 - (\frac{n-1}{2})^2$.

EJEMPLO: Factorizar $n = 6077$.

Se tiene que

$$77 < \sqrt{6077} < 78 \qquad \Rightarrow \qquad t = \left[\sqrt{6077}\right] + 1 = 78$$

Buscamos raíz exacta en

$$\begin{aligned}
78^2 - 6077 &= 6084 - 6077 = 7 \qquad \text{(no tiene raíz entera)} \\
79^2 - 6077 &= 6241 - 6077 = 164 \qquad \text{(no tiene raíz entera)} \\
80^2 - 6077 &= 6400 - 6077 = 323 \qquad \text{(no tiene raíz entera)} \\
81^2 - 6077 &= 6561 - 6077 = 484 = 22^2.
\end{aligned}$$

Entonces

$$6077 = 81^2 - 22^2 = (81-22)(81+22) = 59 \cdot 103,$$

[10]Marin Mersenne (1588-1648)
[11]Pierre de Fermat (1601-1665)

siendo 59 y 103 números primos.

Nota: Como se puede comprobar, éste método también puede resultar muy ineficiente.

DEFINICIÓN 2.2.1

Se conocen como ***números de Fermat*** *a los números de la forma* $F_n = 2^{2^n} + 1$.

Fermat supuso que estos números eran primos. Más tarde Euler demostró que su conjetura era falsa. al comprobar que $F_5 = 2^{2^5} + 1$ no es primo, pues $641|F_5$. De hecho, hasta ahora solo se han comprobado como números primos los 5 primeros números de Fermat; es decir,

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Para demostrar la afirmación anterior nótese que $641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4$. Entonces es

$$\begin{aligned} F_5 = 2^{2^5} + 1 &= 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 5^4)2^{28} + 1 \\ &= 641 \cdot 2^{28} - 5^4 \cdot 2^{28} + 1 = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641 \cdot 2^{28} - (641^4 - 4 \cdot 641^3 + 6 \cdot 641^2 - 4 \cdot 641 + 1) + 1 \\ &= 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4). \end{aligned}$$

Es decir, $641|F_5$.

Por otra parte, se puede demostrar que:

Todo divisor primo de F_n es de la forma $2^{n+2}k + 1$.

Este resultado resulta útil para determinar si un número de Fermat es primo.

EJEMPLO: $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$.

Si un número primo p divide a F_3, entonces es $p = 2^5 k + 1 = 32k + 1$. Además debe ser $p < \sqrt{F_3}$, de donde $32k + 1 < \sqrt{257}$.

$$\begin{aligned} (32k + 1)^2 &< 257 \\ 32^2 k^2 + 64k + 1 &< 257 \\ 32k^2 + 64k - 256 &< 0. \end{aligned}$$

Entonces

$$-1 < -\frac{18}{32} < \frac{-1 - \sqrt{257}}{32} < k < \frac{-1 + \sqrt{257}}{32} < \frac{1}{2} < 1.$$

Es decir, todas las soluciones están en el intervalo $(-1, 1)$, por lo que no hay solución en números primos. Luego, F_3 es primo.

Los números de Fermat demuestran también que existen infinitos números primos.

LEMA 2.2.4 *Para todo n entero se cumple $F_0F_1 \dots F_{n-1} = F_n - 2$.*

Demostración: (Por inducción)

i) Para $n = 1$ se tiene

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3 \\ F_1 - 2 &= (2^{2^1} + 1) - 2 = (2^2 + 1) - 2 = 5 - 2 = 3. \end{aligned}$$

Entonces $F_0 = F_1 - 2$.

ii) Sea $F_0F_1 \dots F_{k-1} = F_k - 2$.

iii) Queremos demostrar que $F_0F_1 \dots F_k = F_{k+1} - 2$.

$$\begin{aligned} F_0F_1 \dots F_k &= (F_0F_1 \dots F_{k-1})F_k = (F_k - 2)F_k \\ &= (2^{2^k} + 1 - 2)(2^{2^k} + 1) = (2^{2^k})^2 - 1 \\ &= 2^{2^{k+1}} - 1 = (2^{2^{k+1}} + 1 - 2) = F_{k+1} - 2. \end{aligned}$$

Q.e.d.

TEOREMA 2.2.3
Si m, n son enteros no negativos diferentes, entonces $(F_n, F_m) = 1$.

Demostración: Sea (sin perder generalidad) $m < n$ y sea $d|F_n$ y $d|F_m$. El Lema 2.2.4 implica que $F_k - F_0F_1 \dots F_m \dots F_{k-1} = 2$, entonces de $n > m$ se deduce que $F_n - F_0F_1 \dots F_m \dots F_{n-1} = 2$.

Además $d|(F_n - F_0F_1 \dots F_{n-1})$, por lo que $d|2$. De aquí que sea $d = 1$ ó $d = 2$. Pero F_n y F_m son impares, por lo que $d \neq 2$. Entonces $d = 1$. **Q.e.d.**

Sabemos que todo F_m tiene divisor primo p_m. El teorema anterior implica que se cumple $p_m \neq p_n$, pues $(F_m, F_n) = 1$. Además existen infinitos números de Fermat F_m. Entonces existen infinitos números primos.

2.2.1. Ejercicios

1. Halle la factorización en números primos de:

   a) 36 b) 222 c) 5040 d) 9999

2. Demuestre que todas las potencias de la factorización prima de n son pares si y sólo si n es un cuadrado perfecto.

3. ¿Cuáles enteros positivos tienen exactamente tres divisores positivos? ¿Cuáles tienen exactamente cuatro?

4. Se conoce que si n es un número entero positivo, entonces la factorización prima de $n!$ es $n! = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, siendo $p_1, p_2, \dots, p_m$ todos los números primos menores o iguales que n y siendo

$$\alpha_k = \left[\frac{n}{p_k}\right] + \left[\frac{n}{p_k^2}\right] + \left[\frac{n}{p_k^3}\right] + \dots \quad \text{para todo} \quad k = 1, 2, \dots m.$$

   a) Encuentre la factorización prima de 20!.

   b) ¿Cuántos ceros hay al final de 1000! en notación decimal?

   c) Encuentra todos los enteros positivos n tales que $n!$ termina exactamente con 74 ceros.

5. Encuentre los enteros a, b tales que $(a, b) = 18$ y $[a, b] = 540$.

6. Demuestre que si p es primo tal que $p^2|a$, entonces $p|a$.

7. Encuentre los enteros a, b tales que $a + b = 798$ y $[a, b] = 10780$.

8. Demuestre que $\sqrt[3]{5}$ es irracional.

9. Factorice

   a) $10^6 - 1$ b) $2^{24} - 1$

10. Usando el método de Fermat factorice

    a) 143 b) 43

11. a) Verifique que F_4 es primo.
    (Sugerencia: Utilice el hecho de que $d|F_4$ si $d = 64k + 1$).

    b) Factorice F_5 usando que $d|F_5$ si $d = 2^7 k + 1$. ($F_5 = 641 \cdot 6700417$)

2.3. Ecuaciones Diofánticas Lineales

Ejemplos de problemas:

1. Un hombre desea adquirir cheques de viajero por 510 USD, pero sólo hay de 20 USD y de 50 USD ¿Cuántos debe comprar de cada tipo?

2. Una mujer desea enviar una carta de 83 centavos, pero sólo hay sellos de 6 y de 15 centavos ¿Cuántos sellos de cada tipo debe comprar?

DEFINICIÓN 2.3.1

Una ecuación en números enteros se llama ***ecuación diofántica****. Por ejemplo, la ecuación* $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ *con* $a_1, a_2, \ldots, a_n, b$ *enteros conocidos y* $x_1, x_2, \ldots, x_n$ *enteros desconocidos, se conoce como* ***ecuación diofántica lineal****.*

Veamos el caso de la ecuación diofántica[12] lineal $ax + by = c$ con $a, b, c \in \mathbb{Z}$ dados.

Sean $x_0, y_0 \in \mathbb{Z}$ solución de la ecuación, entonces es $ax_0 + by_0 = c$. Si $d = (a, b)$, entonces $d|a$ y $d|b$, luego $d|c$. De aquí que

Si $d = (a, b)$ y d no divide a c, entonces $ax + by = c$ no tiene solución.

Por otro lado, si $d|c$ y x_0, y_0 son solución de la ecuación $ax_0 + by_0 = c$, entonces como

$$ax_0 + by_0 = ax_0 + r + by_0 - r = a\left(x_0 + \frac{r}{a}\right) + b\left(y_0 - \frac{r}{b}\right),$$

se tiene que

$$x = x_0 + \frac{r}{a}; \quad y = y_0 - \frac{r}{b}$$

también es solución si $a|r$ y $b|r$, o sea si $r = \frac{ab}{d}n = [a, b]n$. De aquí que:

Si x_0, y_0 son solución de la ecuación $ax + by = c$ con $(a, b)|c$, entonces $x = x_0 + \frac{b}{d}n$; $y = y_0 - \frac{a}{d}n$ con $d = (a, b)$ y $n \in \mathbb{Z}$, también son solución de la ecuación dada.

En general, se cumple el siguiente teorema.

[12]Estas ecuaciones deben su nombre a Diofanto (aproximadamente 250 D.C.), cuya obra cumbre "Arithmetica" es considerada una de las más importantes y llegó a la cúspide de su fama con la edición de Bachet publicada por el hijo de Fermat con sus anotaciones al margen.

TEOREMA 2.3.1

Sean $a, b \in \mathbb{Z}$ tales que $d = (a, b)$. Entonces la ecuación $ax+by = c$ tiene solución si y sólo si $d|c$. En ese caso existen infinitas soluciones, siendo todas *ellas de la forma*

$$\begin{cases} x = x_0 + \frac{b}{d}n \\ y = y_0 - \frac{a}{d}n \end{cases}$$

con x_0, y_0 solución particular de la ecuación dada.

Demostración:

1) Ya vimos que existe solución si y sólo si $d|c$.

2) También vimos que si x_0, y_0 son una solución particular de la ecuación, entonces también lo es

$$\begin{cases} x = x_0 + \frac{b}{d}n \\ y = y_0 - \frac{a}{d}n \end{cases}$$

3) Resta demostrar que si x, y son solución de la ecuación, entonces son de la forma anterior. Sean x_0, y_0 y x, y dos pares de soluciones. Entonces es

$$ax_0 + by_0 = c \quad \text{y} \quad ax + by = c.$$

Entonces $ax + by = ax_0 + by_0$ y, agrupando convenientemente se obtiene

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

Dividiendo por d, es

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \tag{2.1}$$

Pero $(a, b) = d$ implica que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, de donde se deduce que $\frac{a}{d}|(y_0 - y)$ y $\frac{b}{d}|(x - x_0)$, es decir, $y_0 - y = n\frac{a}{d}$ y $x - x_0 = m\frac{b}{d}$. Sustituyendo en (2.1) es $\frac{a}{d}m\frac{b}{d} = \frac{b}{d}n\frac{a}{d}$, o sea $m = n$. Entonces es

$$\begin{cases} x = x_0 + \frac{b}{d}n \\ y = y_0 - \frac{a}{d}n \end{cases}.$$

Q.e.d.

EJEMPLO: $15x + 6y = 7$. Aquí se tiene que $(15, 6) = 3$ y 3 no divide a 7, por lo que la ecuación planteada no tiene solución entera.

EJEMPLO: $21x + 14y = 70$. Aquí se cumple que $(21, 14) = 7|70$, por lo que la ecuación planteada tiene infinitas soluciones enteras. El algoritmo de la división de

Euclides resulta útil para hallarlas, pues basta expresar (a, b) como combinación lineal de a y b. Así es

$$\begin{array}{l} 21 = 1(14) + 7 \\ 14 = 2(7) \end{array},$$

Luego, $d = 7 = 21 - 14$. Multiplicando por 10 es $70 = (10)21 - (10)14$, de donde se obtiene una solución particular

$$x_0 = 10, \qquad y_0 = -10.$$

Entonces, todas las soluciones de la ecuación dada son

$$\begin{cases} x = 10 + \frac{14}{7}n = 10 + 2n \\ y = -10 - \frac{21}{7}n = -10 - 3n \end{cases}.$$

Resolvamos ahora los ejemplos iniciales de la sección.

1. Se debe resolver la ecuación $20x+50y = 510$, donde x, y representan los cheques de viajero de 20 USD y 50 USD respectivamente $(x \geq 0, y \geq 0)$. Aquí se tiene que $(20, 50) = 10|510$, por lo que la ecuación planteada tiene infinitas soluciones enteras que son

   $$\begin{cases} x &= -102 + 5n \\ y &= 51 - 2n \end{cases}.$$

   Pero debe ser $x \geq 0$, o sea $-102 + 5n \geq 0$, lo que implica que $n \geq 20$, es decir $n \geq 21$.

   Si $n = 21$, entonces es

   $$\begin{cases} x &= -102 + 5n = 3 > 0 \\ y &= 51 - 2n = 9 > 0 \end{cases}.$$

   Luego, el hombre debe comprar 3 cheques de 20 USD y 9 cheques de 50 USD.

2. Se debe resolver la ecuación $6x + 15y = 83$, donde x, y representan los sellos de 6 y 15 centavos respectivamente $(x \geq 0, y \geq 0)$.

   Aquí se tiene que $(6, 15) = 3$, pero 3 no divide a 83, por lo que la ecuación planteada no tiene solución entera.

Al generalizar los resultados anteriores se cumple el siguiente teorema.

Teorema 2.3.2

Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tales que $d = (a_1, a_2, \ldots, a_n)$. Entonces la ecuación $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ tiene solución (infinitas) si y sólo si $d|c$.

La demostración (por inducción) se deja como ejercicio al lector.

2.3.1. Ejercicios

1. Solucione:
   a) $2x + 5y = 11$ b) $17x + 13y = 100$
   c) $21x + 14y = 147$ d) $60x + 18y = 97$

2. Un comerciante japonés vuelve a su casa desde los EU y desea cambiar sus dólares americanos y canadienses en yenes. La tasa de cambio en ese momento es de 122 yen por cada dólar norteamericano y 112 yen por cada dólar canadiense. Si recibió en total 13298 yen ¿cuántos dólares de cada tipo cambió?

3. Solucione los sistemas
   a) $\begin{cases} x + y + z &= 100 \\ x + 8y + 50z &= 156 \end{cases}$ b) $\begin{cases} x + y + z &= 100 \\ x + 6y + 21z &= 121 \end{cases}$

4. ¿Es posible juntar con monedas de 1, 10 y 25 centavos la cantidad de 3 pesos, con al menos una moneda de cada denominación?

5. Demostrar el Teorema 2.3.2.

2.4. Ejercicios del capítulo

1. Demuestre que la suma de primos gemelos $p, p+2$ con $p > 3$ siempre es divisible por 12.

2. Demuestre que si n es un número natural que no es divisible por 2 ni por 3, entonces 24 divide a $n^2 + 23$.

3. Demuestre que si $n > 1$ es tal que $a^n - 1$ es primo, entonces tiene que ser $a = 2$ y n primo.

4. Aplicando la identidad $47 = 2^7 - 3^4$ demuestre que 47 divide a $2^{23} - 1$.

5. Demuestre que $\sum_{k=1}^{n} (-1)^{k-1} k^2 = (-1)^{n-1} \frac{n(n+1)}{2}$.

6. Para cada entero positivo n se define

$$T(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ \\ \frac{3n+1}{2} & \text{si } n \text{ es impar} \end{cases}.$$

   Si se forma la sucesión n, $T(n), T(T(n)), T(T(T(n))), \ldots$ iterando T (es decir, $n, T(n), T^2(n), T^3(n), \ldots$) se conjetura que siempre existe un entero positivo k, tal que $T^k(n) = 1$ (esto se conoce como la *Conjetura de Collatz* y aún no ha podido ser demostrado.

a) Encuentre los términos de la sucesión para $n = 39$.

b) Demuestre la Conjetura de Collatz para $n = 2^k$.

c) Demuestre la Conjetura de Collatz para $n = \frac{2^{2k}-1}{3}$

d) Elabore un programa de computación que calcule la sucesión y permita validar la conjetura de Collatz para números diferentes a los de los incisos anteriores.

7. Demuestre que la cuarta potencia de todo entero impar es de la forma $8k + 1$.

8. Demuestre que si p es primo y k es un entero positivo no mayor que p, entonces el coeficiente binomial $\binom{p}{k}$ es divisible por p ¿Qué sucede si p no es primo?

9. a) Demuestre que si a, b, c, d son enteros tales $a, b > 0$ y $\frac{a}{b} + \frac{c}{d}$ es también un número entero y $(a, b) = (c, d) = 1$, entonces es $b = d$.

   b) ¿Qué se puede afirmar si ahora son a, b, c enteros positivos tales que $(a, b) = (c, b) = 1$ y $\frac{1}{a} + \frac{1}{b} + \frac{1}{c}$ es también un número entero?

10. Sea $H = \{n \in \mathbb{Z} : n = 4k + 1 \text{ con } k \geq 0\}$.

    a) Demuestre que el producto de dos elementos de H es siempre un elemento de H.

    b) Un elemento $h \neq 1$ de H se llama **primo hilbertiano** si el único modo de descomponerlo como producto de elementos de H es $h = h \cdot 1 = 1 \cdot h$. Halle los 20 primeros primos hilbertianos.

    c) Demuestre (usando el segundo principio de inducción) que todo elemento de H distinto de 1 puede ser factorizado como producto de primos hilbertianos.

    d) Demuestre, hallando dos factorizaciones distintas de 693, que la factorización de elementos de H en primos hilbertianos no es única.

    e) Elabore un programa de computación para determinar los n primeros primos hilbertianos.

11. Un antiguo juego chino del siglo VI conocido como *"el juego de las aves"* y creado por el matemático Chang Chíu-chen, plantea: Si un gallo vale 5 monedas, una gallina vale 3 monedas y tres pollos juntos valen una moneda y se desean comprar 100 de estas aves en total. ¿Cuántos de cada tipo se pueden comprar con 100 monedas?

12. Halle todos los números enteros x, y que satisfacen la ecuación diofántica

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

13. Demuestre que si a y b son enteros, con $b > 0$, entonces existen enteros únicos q y r que satisfacen $a = qb + r$ con $2b \leq r < 3b$.

14. Demuestre que todo entero de la forma $6k + 5$ es también de la forma $3k' + 2$, pero el recíproco no es válido.

15. Use el algoritmo de la división para comprobar que

    a) todo entero impar es de la forma $4k + 1$ ó $4k + 3$.

    b) el cuadrado de todo entero es de la forma $3k$ ó $3k + 1$.

    c) el cubo de todo entero es de la forma $9k$, $9k + 1$ ó $9k + 8$.

16. Para $n \geq 1$, demuestre que $n(n + 1)(2n + 1)/6$ es entero. (Sugerencia: Aplique el algoritmo de la división con $b = 6$.)

17. Compruebe que si un entero es simultáneamente cuadrado y cubo perfecto (como en el caso de $64 = 8^2 = 4^3$), entonces tiene que ser de la forma $7k$ ó $7k + 1$.

18. Obtenga la siguiente versión del algoritmo de la división: Dados dos enteros a y b, con $b \neq 0$, existen únicos enteros q y r, tales que $a = qb+r$ y $-\frac{1}{2}|b| \leq r < \frac{1}{2}|b|$.

19. Demuestre que ningún entero en la sucesión $11, 111, 1111, 11111 \ldots$ es un cuadrado perfecto. (Sugerencia: compruebe que todo término de esa sucesión es de la forma $4k + 3$.)

20. Si $a|b$, demuestre que $-a|b$, $a| - b$ y $-a|(-b)$.

21. Dados tres enteros a, b, c, demuestre que

    a) si $a|b$, entonces $a|bc$.

    b) si $a|b$ y $a|c$, entonces $a^2|bc$.

    c) si $a|b$ si y sólo si $ac|bc$ con $c \neq 0$.

22. Demuestre que para todo entero a, uno de los enteros a, $a+2$, $a+4$ es divisible por 3. (Sugerencia: mediante el algoritmo de la división se puede determinar la forma de a.)

23. *a*) Para un entero cualquiera a, compruebe que $2|a(a+1)$ y $3|a(a+1)(a+2)$.

    b) Demuestre que $4 \nmid (a^2 + 2)$ para cualquier entero a.

24. Utilice la inducción para comprobar que para $n \geq 1$ se cumple

    a) $7|2^{3n} - 1$ y $8|3^{2n} + 7$.

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

25. Demuestre que si a es un entero tal que $2 \nmid a$ y $3 \nmid a$, entonces $24|(a^2 - 1)$.

26. Demuestre que

    a) la suma de los cuadrados de dos enteros impares no puede ser un cuadrado perfecto.

    b) el producto de cuatro enteros consecutivos es menor en 1 que un cuadrado perfecto.

27. Compruebe que la diferencia de dos cubos consecutivos nunca es divisible por 2.

28. Dado un entero no nulo a, demuestre que $(a, 0) = |a|$, $(a, a) = |a|$ y $(a, 1) = 1$.

29. Si a y b son enteros no simultáneamente nulos, demuestre que

$$(a, b) = (-a, b) = (a, -b) = (-a, -b).$$

30. Demuestre que dados un entero positivo n y un entero cualquiera a, se cumple que $(a, a + n)|n$, de donde se deduce que $(a, a + 1) = 1$.

31. Dados dos enteros a y b demuestre que

    a) existen enteros x, y tal que $c = ax + by$ si y sólo si $(a, b)|c$.

    b) si existen enteros x, y tal que $ax + by = (a, b)$, entonces $(x, y) = 1$.

32. Demuestre que el producto de tres enteros consecutivos cualesquiera es divisible por 6, el producto de cuatro enteros consecutivos cualesquiera es divisible por 24 y el producto de cinco enteros consecutivos cualesquiera es divisible por 120 (Sugerencia: Aplique el segundo corolario del teorema sobre la representación de (a, b) como combinación lineal de a, b).

33. Demuestre cada una de las siguientes afirmaciones

    a) Si a es un entero impar, entonces $24|a(a^2 - 1)$ (Sugerencia: el cuadrado de un entero impar es de la forma $8k + 1$).

    b) Si a y b son enteros impares, entonces $8|(a^2 - b^2)$.

    c) Si a es un entero no divisible por 2 y 3, entonces $24|(a^2 + 23)$ (Sugerencia: todo entero a tiene una de las formas $6k$, $8k + 1$,. . . , $6k + 5$).

    d) Si a es un entero cualquiera, entonces $360|a^2(a^2 - 1)(a^2 - 4)$.

34. Demuestre las siguientes propiedades del máximo común divisor

    a) Si $(a, b) = 1$ y $(a, c) = 1$, entonces $(a, bc) = 1$ (Sugerencia: como se cumple $1 = ax + by = au + cv$ para ciertos x, y, u, v, entonces

$$1 = (ax + by)(au + cv) = a(aux + cvx + byu) + bc(yv)).$$

b) Si $(a,b)=1$ y $c|a$, entonces $(b,c)=1$.

c) Si $(a,b)=1$ y $(a,c)=1$, entonces $(ac,b)=(c,b)$.

d) Si $(a,b)=1$ y $c|(a+b)$, entonces $(a,c)=(b,c)=1$. (Sugerencia: sea $d=(a,c)$, entonces $d|a$ y $d|c$ implica que $d|(a+b)-a$ ó $d|b$).

35. Halle $(143,227)$, $(306,657)$ y $(272,1479)$.

36. Utilice el algoritmo de Euclides para obtener enteros x,y de modo que se cumpla $ax+by=(a,b)$ para:

a) $a=56, \quad b=72$.

b) $a=24, \quad b=138$.

c) $a=119, \quad b=272$.

d) $a=1769, \quad b=2378$.

37. Demuestre que si d es divisor común de a y b, entonces $d=(a,b)$ si y sólo si $\left(\frac{a}{d},\frac{b}{d}\right)=1$. (Sugerencia: utilice el teorema que relaciona (a,b) con $[a,b]$.)

38. Si $(a,b)=1$, demuestre que

a) $(a+b,a-b)=1$ ó $(a+b,a-b)=2$ (Sugerencia: para $d=(a+b,a-b)$, compruebe que $d|2a$ y $d|ab$, de donde $d\leq(2a,2b)=2(a,b)$).

b) $(2a+b,a+2b)=1$ ó $(2a+b,a+2b)=3$.

c) $(a+b,a^2+b^2)=1$ ó $(a+b,a^2+b^2)=2$ (Sugerencia: utilice la identidad $a^2+b^2=(a+b)(a-b)+2b^2$).

d) $(a+b,a^2-ab+b^2)=1$ ó $(a+b,a^2-ab+b^2)=3$ (Sugerencia: utilice que $a^2-ab+b^2=(a+b)^2-3ab$).

39. Para enteros positivos a,b y $n\geq 1$ demuestre que

a) si $(a,b)=1$, entonces $(a^n,b^n)=1$ (Sugerencia: ver problema 16 a) de la sección anterior).

b) la relación $a^n|b^n$ implica que $a|b$ (Sugerencia: hacer $d=(a,b)$ y escribir $a=rd$, $b=sd$, con $(r,s)=1$; por a) se tiene $(r^n,s^n)=1$, compruebe que $r=1$, de donde $a=d$).

40. Demuestre que si $a\geq 2$ y a^n+1 es primo, entonces a es par y n es una potencia de 2.

41. Demuestre que los números $2^{2^n}+1$ $(n=0,1,2,\ldots)$ son primos relativos dos a dos y deduzca de ello una nueva demostración del teorema 2.1.8 (G.Polya).

42. Si a,b,n son números naturales, demuestre que $(n^a-1,n^b-1)=n^{(a,b)}-1$, aplicando el algoritmo de Euclides.

43. Demuestre que si a, b, c, d son números naturales con $ab = cd$, entonces (Lauffer)

$$a = \frac{(a,c)(a,d)}{(a,b,c,d)}.$$

44. Sean $n, n_1, n_2 \in \mathbb{N}$ con $n|n_1n_2$, pero $n \nmid n_1$ y $n \nmid n_2$. Demuestre que (Sierpinski)

$$d = \frac{n_1}{\left(n_1, \frac{n_1n_2}{n}\right)}$$

es un divisor de n con $1 < d < n$.

45. Un polinomio $P(x)$ con coeficientes reales se dice *entero*, si $P(n) \in \mathbb{Z}$ para todo entero n. Demuestre que todo polinomio entero se puede representar de modo único como

$$P(x) = a_0 + a_1\binom{x}{1} + a_2\binom{x}{2} + \ldots + a_n\binom{x}{n}.$$

coeficientes enteros

46. Sea $P(x)$ un polinomio entero. Demuestre que no todos los elementos de la sucesión $\{P(n)\}_{n=0}^{\infty}$ pueden ser números primos. Considere en particular el ejemplo $P(x) = 2\binom{x}{2} + 41$. (Sugerencia: Para un demostración directa analice $P(0) = p$ y halle un número natural x tal que $P(x) > p$ y $p|P(x)$.)

47. En el juego de Euclides juegan dos personas e inician el juego con un par de enteros positivos $\{x, y\}$ según las reglas siguientes:

    - Se puede mover del par $\{x, y\}$ a un par cualquiera del tipo $\{x - ty, y\}$ siempre que $x - ty \geq 0$.
    - Gana el jugador que logre obtener un par de la forma $\{0, y\}$.

    Demuestre que toda sucesión de movimientos iniciada con un par $\{a, b\}$ termina (a lo sumo) en el par $\{0, (a, b)\}$.

48. Para enteros no nulos a, b demuestre que son equivalentes las siguientes condiciones

$$a|b \qquad \Leftrightarrow \qquad (a,b) = |a| \qquad \Leftrightarrow \qquad [a,b] = |b|.$$

49. Halle $[143, 227]$, $[306, 657]$ y $[272, 1479]$.

50. Demuestre que el máximo común divisor de dos enteros positivos siempre divide a su mínimo común múltiplo.

51. Dados enteros no nulos a, b demuestre los siguientes resultados relativos a $[a, b]$

    a) $(a, b) = [a, b]$ si y sólo si $a = b$.

b) Si $k > 0$, entonces $[ka, kb] = k[a, b]$.

c) Para cualquier múltiplo común m de a y b es $[a, b]|m$ (Sugerencia: para $t = [a, b]$ aplique el algoritmo de la división para obtener $m = qt + r$ con $0 \leq r < t$, compruebe que r es múltiplo común de a y b).

52. Sean a, b, c enteros de modo que no se anulen simultáneamente dos de ellos y sea $d = (a, b, c)$. Demuestre que

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

53. Encuentre enteros x, y, z tal que $(198, 288, 512) = 198x + 288y + 512z$ (Sugerencia: sea $d = (198, 288)$. Como $(198, 288, 512) = (d, 512)$, encuentre primero enteros u, v tal que $(d, 512) = du + 512v$).

54. Determine todas las soluciones enteras de las siguientes ecuaciones diofánticas

a) $56x + 72y = 40$

b) $24x + 138y = 18$

c) $221x + 91y = 117$

d) $84x - 438y = 156$

55. Determine todas las soluciones enteras positivas de las siguientes ecuaciones diofánticas

a) $30x + 17y = 300$

b) $54x + 21y = 906$

c) $123x + 360y = 99$

d) $158x - 57y = 7$

56. Si a, b son enteros positivos primos relativos, demuestre que la ecuación diofántica $ax - by = c$ tiene infinitas soluciones en lo enteros positivos.

57. *a*) Demuestre que la ecuación diofántica $ax + by + cz = d$ tiene solución en los enteros si y sólo si $(a, b, c)|d$.

b) Halle todas las soluciones enteras de $15x + 12y + 30z = 24$ (Sugerencia: hacer $y = 3s - 5t$ and $x = -s + 2t$).

58. *a*) Un hombre dispone de $\$4,55$ compuesto totalmente de monedas de 10 y 25 centavos. ¿Cuál es el mayor y menor número de monedas que puede tener? ¿es posible que tenga igual cantidad de monedas de 10 y de 25 centavos?

b) El teatro del barrio cuesta \$1,80 para adultos y 75 centavos para los niños. En cierta tarde la entada total fue de \$90. Si se conoce que había más adultos que niños ¿cuántas personas asistieron ese día?

c) Se suman una cierta cantidad de 6 y de 9 para obtener una suma de 126. Si se intercambian las cantidades de 6 y 9 la suma resulta 11. ¿qué cantidad de cada número había originalmente?

59. Un granjero compró cien cabezas de ganado con un costo total de $4000. Los precios por cabeza de ganado eran como sigue: los terneros $120; los corderos $50; los cerdos $25. Si el granjero obtuvo al menos un animal de cada tipo ¿cuántos de cada tipo compró?

60. Cuando Mr. Smith cobró un cheque en su banco, el cajero confundió el el número de centavos con el número de pesos. Sin haberlo notado, Mr. Smith gastó 68 centavos y entonces notó para su sorpresa que tená el doble de la cantidad del cheque original. Determine el valor más pequeño para el que podría haber sido escrito el cheque (Sugerencia: Si x es el número de pesos e y el número de centavos en el cheque, entonces es $100y + x - 68 = 2(100x + y)$).

61. Se conjetura que existen infinitos primos de la forma $n^2 - 2$. Encuentre 5 de esos primos.

62. Demuestre con un ejemplo la falsedad de la siguiente conjetura: Todo entero positivo puede ser escrito en la forma $p + a^2$, donde p es primo ó 1 y $a \geq 0$.

63. Demuestre las siguientes proposiciones

    a) Todo primo de la forma $3n + 1$ es también de la forma $6n + 1$.

    b) Todo entero de la forma $3n + 2$ tiene un factor primo de esa forma.

    c) El único primo de la forma $n^3 - 1$ es 7 (Sugerencia: escriba $n^3 - 1$ como $(n - 1)(n^2 + n + 1)$).

    d) El único primo p para el que $3p - 1$ es un cuadrado perfecto es $p = 5$.

64. Si $p > 5$ es un número primo, compruebe que $p^2 + 2$ es compuesto (Sugerencia: p tiene una de las formas $6k + 1$ ó $6k + 5$).

65. *a*) Si p es primo y $p|a^n$, demuestre que $p^n|a^n$.

    b) Si $(a, b) = p$ ¿cuáles son los valores posibles de (a^2, b^2), (a^2, b) y (a^3, b^2)?

66. Demuestre las siguientes proposiciones

    a) Todo entero de la forma $n^4 + 4$ con $n > 1$ es compuesto.

    b) Si $n > 4$ es compuesto, entonces $n|(n - 1)!$.

    c) Todo entero de la forma $8^n + 1$ con $n \geq 1$ es compuesto (Sugerencia: note que $2^n + 1|2^{3n} + 1$).

67. Halle todos los números primos que dividen a 50!.

68. Si $p \geq q \geq 5$ y p y q son primos, demuestre que $24|p^2 - q^2$.

69. *a*) Una pregunta abierta es la referida a la existencia de infinitos primos que exceden en 1 a una potencia de 2, tales como $5 = 2^2 + 1$. Encuentre dos más de esos primos.

    b) Una conjetura más general plantea que existen infinitos primos de la forma $n^2 + 1$, por ejemplo, $257 = 16^2 + 1$. Encuentre 5 primos más de ese tipo.

70. Si $p \neq 5$ es primo impar, demuestre que $p^2 - 1$ ó $p^2 + 1$ es divisible por 10 (Sugerencia: p toma una de las formas $5k + 1$, $5k + 2$, $5k + 3$ ó $5k + 4$).

71. Otra conjetura no demostrada es la referida a la existencia de infinitos primos que son menores en 1 que una potencia de 2, tales como $3 = 2^2 - 1$.

    a) Encuentre cuatro más de esos primos.

    b) Si $2^k - 1$ es primo, muestre que k es un entero impar, excepto cuando $k = 2$ (Sugerencia: $3|4^n - 1$ para todo $n \geq 1$).

72. Halle la factorización prima de los enteros 1234, 10140 y 36000.

73. Considere el conjunto S de todos los enteros positivos de la forma $3k + 1$, es decir, $S = (1, 4, 7, 10, 13, 16, \ldots)$. Un entero $a > 1$ de S se dice primo si no puede ser factorizado en dos enteros menores, ambos de S (así 10 y 25 son primos, mientras que $16 = 4 \cdot 4$ y $28 = 4 \cdot 7$ no lo son).

    a) Demuestre que cada elemento de S es primo o producto de primos.

    b) Dé un ejemplo que muestre que un entero de S puede ser factorizado en primos es más de un modo.

74. Se conjetura que todo entero puede ser escrito como la diferencia de dos primos consecutivos de infinitas maneras. Por ejemplo,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013.$$

    Exprese el entero 10 como diferencia de dos primos consecutivos de 15 maneras diferentes.

75. Demuestre que un entero positivo $a > 1$ es un cuadrado si y sólo si en la forma canónica de a todos los exponentes de los primos son pares.

76. Un entero se dice libre de cuadrado si no es divisible por el cuadrado de ningún entero mayor que 1. Demuestre que

    a) un entero $n > 1$ es libre de cuadrado si y sólo si n puede ser factorizado como producto de primos diferentes;

b) todo entero $n > 1$ es el producto de un entero libre de cuadrado y una cuadrado perfecto. (Sugerencia: Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ es la factorización canónica de n, escriba $k_i = 2q_i + r_i$, donde $r_i = 0$ ó $r_i = 1$ de acuerdo a que k sea par o impar).

77. Compruebe que todo entero n puede ser expresado como $n = 2^k m$, donde $k \geq 0$ y m es un entero impar.

78. La evidencia numérica hace suponer que existen infinitos primos tales que $p + 50$ es también primo. Halle 15 de esos primos.

79. Determine si el entero 701 es primo, comprobando todos los primos $p \leq \sqrt{701}$ como posibles divisores. Haga lo mismo para 1009.

80. Con la ayuda de la criba de Eratosthenes obtenga todos los números primos entre 100 y 200.

81. Dado que $p \nmid n$ para todo primo $p \leq \sqrt[3]{n}$, demuestre que n es primo o es producto de dos primos (Sugerencia: Asuma que n tiene 3 factores primos).

82. Demuestre que:

a) $\sqrt{p}$ es iracional para todo primo p.

b) Si $a > 0$ y $\sqrt[n]{a}$, entonces $\sqrt[n]{a}$ tiene que ser entero.

c) Para $n \geq 2$, $\sqrt[n]{n}$ es irracional (Sugerencia: utilice que $2^n > n$).

83. Demuestre que todo número compuesto de tres dígitos tiene que tener un factor primo menor o igual que 31

84. Complete los detalles faltantes en este esquema de demostración de la infinitud de los números primos: Asuma que existen sólo finitos primos $p_1, p_2, \ldots, p_n$. Sea A el producto de cualesquiera r de esos primos y sea

$$B = \frac{p_1 \cdot p_2 \cdots p_n}{A}.$$

Entonces todo p_k divide a A o a B, pero no a ambos a la vez. Como $A + B > 1$, entonces $A + B$ tiene que tener un divisor primo diferente de los p_k, una contradicción.

85. Modifique la demostración de Euclides de la infinitud de los primos, asumiendo la existencia de un mayor primo p y usando al entero $N = p! + 1$ para llegar a una contradicción.

86. Dé otra prueba de la infinitud de los primos, asumiendo la existencia finitos primos $p_1, p_2, \ldots, p_n$ y usando al entero

$$N = p_2 \cdot p_3 \cdots p_n + p_1 \cdot p_3 \cdots p_n + \ldots + p_1 \cdot p_2 \cdots p_{n-1}$$

para llegar a una contradicción.

87. Demuestre que si $n > 2$, entonces existe un primo p que satisface la relación $n < p < n!$ (Sugerencia: Si $n! - 1$ no es primo, entonces tiene un divisor primo p; $p \leq n$ implica que $p|n!$, lo que conduce a una contradicción).

88. Si p_n denota al n-ésimo número primo, demuestre que ninguno de los enteros

$$P_n = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

es un cuadrado perfecto. (Sugerencia: cada P_n es de la forma $4k + 3$).

89. Compruebe que los enteros 1949 y 1951 son primos gemelos.

90. *a*) Si se adiciona 1 al producto de primos gemelos, demuestre que siempre se obtiene un cuadrado perfecto.

    b) Demuestre que la suma de primos gemelos p y $p + 2$ es divisible por 12, siempre que $p > 3$.

91. Encuentre todos los pares de primos p, q que satisfacen $p - q = 3$.

92. Sylvester (1896) reformuló la conjetura de Goldbach como sigue: Todo entero para $2n$ mayor que 4 es la suma de dos primos, uno mayor que $\frac{n}{2}$ y el otro menor que $\frac{3n}{2}$. Verifique esta versión de la conjetura para todos los enteros pares entre 6 y 76.

93. En 1752 Goldbach envió la siguiente conjetura a Euler: Todo entero impar puede ser escrito en la forma $p + 2a^2$, donde p es primo o 1 y $a \geq 0$. Compruebe que el entero 5777 refuta la conjetura.

94. Demuestre que la conjetura de Goldbach de que todo entero par mayor que 4 es suma de dos primos implica que todo entero mayor que 5 es suma de tres primos. Esta segunda proposición se conoce como *conjetura débil de Goldbach*. (Sugerencia: Si $2n-2 = p_1+p_2$, entonces $2n = p_1+p_2+2$ y $2n+1 = p_1+p_2+3$).

95. Una conjetura de Lagrange (1775) afirma que todo entero impar mayor que 5 puede ser escrito como suma $p_1 + 2p_2$, siendo p_1, p_2 primos. Confirme esto para los enteros impares hasta 75.

96. Dado un entero positivo n, se puede comprobar que existe un entero par que se puede representar como suma de dos primos impares de n maneras diferentes. Compruebe que los enteros 60, 78 y 84 pueden ser escritos como sumas de dos primos en seis, siete y ocho maneras respectivamente.

97. *a*) Para $n > 3$ muestre que los enteros n, $n + 2$ y $n + 4$ no pueden ser primos a la vez.

    b) Tres primos de la forma $p, p + 2, p + 6$ son llamados primos trillizos. Halle cuatro conjuntos de primos trillizos.

98. Demuestre que la sucesión

$$(n+1)!-2, (n+1)!-3, \ldots, (n+1)!-(n+1)$$

produce n enteros compuestos consecutivos.

99. Halle el menor entero positivo n para los que la función $f(n) = n^2 + n + 17$ es compuesto. Investigue o mismo para las funcines $g(n) = n^2 + 21n + 1$ y $h(n) = 3n^2 + 3n + 23$.

100. El siguiente resultado fue conjeturado por Bertrand, pero el primero en demostrarlo fue Tchebychef en 1850: Para todo entero positivo $n > 1$, existe al menos un primo p que satisface $n < p < 2n$. Use la conjetura de Bertrand para mostrar que $p_n < 2^n$, donde p es el n-ésimo primo.

101. Aplique el mismo método del teoprema 2.1.11 para demostrar que existen infinitos primos de la forma $6n + 5$.

102. Halle un divisor primo del entero $N = 4(3 \cdot 7 \cdot 11) - 1$ de la forma $4n + 3$. Haga lo mismo para $N = 4(3 \cdot 7 \cdot 11 \cdot 15) - 1$.

103. Otra pregunta abierta es cuándo existe un número infinito de conjunto de cinco enteros consecutivos de los cuales cuatro son primos. Encuentre cinco de esos conjuntos.

104. Sea la sucesión de primos, con el 1, denotada por $p_0 = 1$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$. Para cada $n \geq 1$ se conoce que existe una selección adecuada de coeficientes $\varepsilon_k = \pm 1$ tal que

$$p_{2n} = p_{2n-1} + \sum_{k=0}^{2n-2} \varepsilon_k p_k, \qquad p_{2n+1} = 2p_{2n} + \sum_{k=0}^{2n-1} \varepsilon_k p_k.$$

Por ejemplo,

$$13 = 1 + 2 - 3 - 5 + 7 + 11 \qquad \text{y} \qquad 17 = 1 + 2 - 3 - 5 + 7 - 11 + 2 \cdot 13.$$

Halle representaciones similares para los primos 23, 29, 31 y 37.

105. En 1848 de Polignac planteó que todo entero impar es la suma de un primo y una potencia de 2. Por ejemplo, $55 = 47 + 2^3 = 23 + 2^5$. Demuestre que los enteros 509 y 877 refutan dicha afirmación.

106. *a*) Si p es primo y $p \nmid b$, demuestre que en la progresión aritmética

$$a, a + b, a + 2b, \ldots$$

el p-ésimo término es divisible por p (Sugerencia: Como $(p, b) = 1$, existen enteros r, s tal que $1 = pr + bs$. Haga $n_k = kp - as$ para $k = 1, 2, \ldots$ y demuestre que $p|(a + n_k b)$).

b) Partiendo de a) concluya que si b es un entero impar, entonces todo otro término de la progresión es par.

107. En 1950 se demostró que todo entero $n > 9$ puede ser escrito como suma de distintos primos impares. Exprese los enteros 25, 69, 81 y 125 de ese modo.

108. Si p y $p + 8$ son primos, demuestre que $p^3 + 4$ también es primo.

109. *a*) Para todo entero $k > 0$ compruebe que la progresión aritmética

$$a, a + b, a + 2b, \ldots,$$

donde $(a, b) = 1$ contiene k términos consecutivos que son compuestos (Sugerencia: sea $n = (a + b)(a + 2b) \cdots (a + kb)$ y considere los k términos

$$a + (n + 1), a + (n + 2)b, \ldots, a + (n + k)b.$$

b) Halle cinco términos consecutivos compuestos en la progresión aritmética $6, 11, 16, 21, 26, 31, 36, \ldots$

110. Demuestre que 13 es el mayor primo que puede dividir dos enteros sucesivos de la forma $n^2 + 3$.

111. *a*) La media aritmética de los primos gemelos 5 y 7 es el número triangular 6 ¿existe alguna otra pareja de primos gemelos con media aritmética triangular?

b) La media aritmética de los primos gemelos 3 y 5 es el cuadrado perfecto 4 ¿existe alguna otra pareja de primos gemelos con media aritmética cuadrada?

112. Determine todos los primos gemelos p y $q = p+2$ para los que $pq-2$ es también primo.

113. Use el método de Fermat para factorizar

a) 2279

b) 10541

c) 340663 (Sugerencia: el menor cuadrado que excede a 340663 es 587^2).

114. Demuestre que un cuadrado perfecto debe terminar en los siguientes pares de dígitos:

$$00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96.$$

(Sugerencia: como $x^2 \equiv (50 + x)^2 (mod\ 100)$ y $x^2 \equiv (50 - x)^2 (mod\ 100)$, basta examinar los dígitos finales de x^2 para los 25 valores $x = 0, 1, 2, ..., 25$).

115. Factorice el número $2^{11} - 1$ por el método de factorización de Fermat.

116. En 1647, Mersenne notó que cuando un número puede ser escrito como suma de dos cuadrados primos relativos en dos formas distintas, es compuesto y puede ser factorizado en la siguiente forma: Si $n = a^2 + b^2 = c^2 + d^2$, entonces

$$n = \frac{(ac + bd)(ac - bd)}{(a + d)(a - d)}.$$

Use ese resultado para factorizar los números

$$493 = 18^2 + 13^2 = 22^2 + 3^2$$

y

$$38025 = 168^2 + 99^2 = 156^2 + 117^2.$$

Capítulo 3

CONGRUENCIAS

3.1. El príncipe

La teoría de congruencias o aritmética de restos ofrece otro acercamiento a los temas de divisibilidad. El concepto y la notación que empoderan como herramienta a la teoría de congruencias, fueron desarrollados por el matemático alemán Karl Friedrich Gauss (1777-1855) en su monumental obra "Disquisitiones Arithmeticae", que publicó en 1801 con solo 24 años de edad. Respecto a ese gran matemático dijo Kronecker:

> "*Es realmente asombroso, pensar que un solo hombre de tal juventud pudiera ser capaz traer a la luz semejante riqueza de resultados, y sobre todo de presentar semejante el tratamiento profundo y bien organizado de una disciplina completamente nueva.*"

La aptitud natural de Gauss para los números se mostró a la temprana edad de tres años. cuando corrigió un error de suma en los cálculos de su padre. Una de sus mas famosas anécdotas refiere que al asistir con 6 años de edad a su primera clase de Aritmética, el maestro propuso la tarea de sumar todos los números del 1 al 100. No había transcurrido un minuto cuando Gauss provocó su asombro con la respuesta correcta 5050. El joven había reconocido que podía agrupar los números en 50 parejas que suman 101, seleccionando cada vez al menor y al mayor de todos. Con esa misma técnica se obtiene también la ya conocida fórmula de la suma de los n primeros enteros positivos

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

Con 17 años en 1796 Gauss se decidió por el estudio de la Matemática al lograr resolver un problema que permanecía abierto desde la Antigüedad: demostró que el polígono regular de 17 lados se puede construir utilizando solamente regla y compás.

En 1799 Gauss dedicó su tesis doctoral al desarrollo de su primera demostración rigurosa del Teorema Fundamental del Álgebra, que plantea que todo polinomio de

grado n tiene exactamente n raíces complejas. A lo largo de su vida publicó varias demostraciones diferentes de este teorema.
Pero no solo la Matemática fue fuente de su merecida fama. En el área de la Astronomía Gauss logró calcular la órbita de Ceres con asombrosa exactitud, lo cual provocó su nombramiento como director del Observatorio de Gottingen.

Cuando la Ciencia Matemática había crecido, ampliando en gran medida sus campos, era cada vez más difícil dominarla en su totalidad. Los estudios de Gaus fueron tan variados que muchos historiadores lo consideran el último matemático general y es llamado "Princeps Mathematicorum" (Príncipe de las Matemáticas). Aunque Gauss estudió diversas ramas de la Matemática, siempre se destacó en la Teoría de Números y ha llegado a nuestros días su famosa frase

> "*La Matemática es la Reina de las Ciencias, y la Aritmética es la Reina de la Matemática.*"

En el primer capítulo de "Disquisitiones Arithmeticae" Gauss introduce el concepto de congruencia y explica que decide usar la notación "$\equiv$" por su parecido a la igualdad algebraica.

3.2. El concepto de congruencia

Definición 3.2.1

Sean a, b, m números enteros ($m > 0$). Se dice que a ***es congruente a*** *b* ***módulo*** *m, si m divide a $a - b$.* Notación*: $a \equiv b (mod\ \ m)$.*

EJEMPLO: $22 \equiv 4 (mod\ \ 9)$ pues $22 - 4 = 18$ y $9|18$. Pero $13 \not\equiv 5 (mod\ \ 9)$, pues 9 no divide a $8 = 13 - 5$.

Teorema 3.2.1

Si a, b, m son números enteros ($m > 0$) tales que $a \equiv b\ (mod\ m)$, entonces existe un número entero k tal que $a = km + b$.

Demostración: Si $a \equiv b (mod\ m)$, entonces m divide a $a - b$. De aquí que existe un número entero k tal que $a - b = km$, lo cual demuestra el teorema. **Q.e.d.**

A continuación se presentan algunas propiedades básicas de las congruencias.

TEOREMA 3.2.2

La congruencia módulo m ($m > 0$) es una ***relación de equivalencia****. Es decir, para cualesquiera enteros a, b, c se cumplen las propiedades de*

i) ***Reflexividad****, o sea $a \equiv a(mod\ m)$*

ii) ***Simetría****, o sea si $a \equiv b(mod\ m)$, entonces es $b \equiv amod\ m)$*

iii) ***Transitividad****, o sea, si $a \equiv b(mod\ m)$, y $b \equiv c(mod\ m)$, entonces es $a \equiv c(mod\ m)$.*

Demostración:

i) Es obvio que $a - a = 0$ y $m|0$, de donde es $a \equiv a(mod\ m)$.

ii) Si $a \equiv b(mod\ m)$, entonces se tiene que $m|(a - b)$. De aquí que $m|(b - a)$, es decir $b \equiv a(mod\ m)$.

iii) Si $a \equiv b(mod\ m)$, y $b \equiv c(mod\ m)$, entonces $m|(a - b)$ y $m|(b - c)$. Pero $(a - b) + (b - c) = a - c$, por lo que $m|(a - c)$, de donde $a \equiv c(mod\ m)$.**Q.e.d.**

De este teorema se deduce que:

La congruencia módulo m produce una partición del conjunto $\mathbb{Z}$ de los números enteros en m clases de equivalencia, siendo la clase del entero a el conjunto

$$\overline{a} = \{b \in \mathbb{Z} : b \equiv a(mod\ b)\}.$$

EJEMPLO: Las 4 clases de equivalencia de la congruencia módulo 4 son

$$\begin{aligned}
\overline{0} &= \{n \in \mathbb{Z} : n \equiv 0(mod\ 4)\} = \{0, \pm 4, \pm 8, \pm 12, \ldots\} \\
\overline{1} &= \{n \in \mathbb{Z} : n \equiv 1(mod\ 4)\} = \{\pm 1, \pm 5, \pm 9, \pm 13, \ldots\} \\
\overline{2} &= \{n \in \mathbb{Z} : n \equiv 2(mod\ 4)\} = \{\pm 2, \pm 6, \pm 10, \pm 14, \ldots\} \\
\overline{3} &= \{n \in \mathbb{Z} : n \equiv 3(mod\ 4)\} = \{\pm 3, \pm 7, \pm 11, \pm 15, \ldots\}.
\end{aligned}$$

Con ello se obtiene en el anillo $\mathbb{Z}$ una partición en clases de equivalencia $\mathbb{Z}/_{R_m}$.

DEFINICIÓN 3.2.2

Clase de restos módulo *m es $\overline{a} = \{x \in \mathbb{Z};\ x \equiv a(mod\ m)\}$.*

Entonces $\mathbb{Z}/_{R_m}$ está formado por todas las clases de restos módulo m, por lo que tiene m elementos.

Del teorema 3.2.1 se deduce que:

Todo entero es congruente módulo m a su resto en la división por m.

DEFINICIÓN 3.2.3

Si $a = km + r$ con $0 \leq r < a$ (es decir $a \equiv r(mod\ m)$), entonces r se conoce con el nombre de ***menor residuo no negativo de*** *a* ***módulo*** *m y se denota por $r = a_{mod\ m}$.*

EJEMPLO: $17_{mod\ 5} = 2$, pues $17 = 3(5) + 2$ y $-8_{mod\ 7} = 6$, pues $-8 = -2(7) + 6$.

DEFINICIÓN 3.2.4

Los enteros $a_1, a_2, \ldots, a_m$ constituyen un ***sistema completo de restos módulo*** *m si para todos $i \neq j$ se cumple $a_i \not\equiv a_j (mod\ m)$.*

Por ejemplo, un sistema completo de restos módulo m es siempre

$$\{0, 1, 2, \ldots, m-1\}.$$

Así mismo, si m es un número impar, entonces el conjunto

$$\left\{0, \pm 1, \pm 3, \ldots, \pm\frac{m-3}{2}, \pm\frac{m-1}{2}\right\}$$

es también un sistema completo de restos módulo m, que se conoce con el nombre de **conjunto de los menores residuos absolutos módulo** m.

Entonces se puede describir a $\mathbb{Z}/_{R_m}$ por $\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

PROPIEDADES DEL CÁLCULO DE CONGRUENCIAS

TEOREMA 3.2.3

Si a, b, c, m son números enteros $(m > 0)$ y $a \equiv b(mod\ m)$, entonces es

i) $a \pm c \equiv b \pm c(mod\ m)$

ii) $ac \equiv bc(mod\ m)$.

Demostración: Si $a \equiv b(mod\ m)$, entonces $m|(a-b)$.

i) De aquí que $m|(a-b+c-c) = (a+c)-(b+c)$, de donde $a+c \equiv b+c(mod\ m)$. De modo análogo se observa que $a - c \equiv b - c(mod\ m)$.

ii) Se tiene que $a - b = km$ para algún valor entero k. Entonces se cumple que $c(a-b) = ckm = qm$, es decir $m|(ca - cb)$, de donde $ac \equiv bc(mod\ m)$. **Q.e.d.**

EJEMPLO: Como $19 \equiv 3(mod\ 8)$, entonces es $19 + 7 \equiv 3 + 7(mod\ 8)$, es decir $26 \equiv 10 \equiv 2(mod\ 8)$.

En $\mathbb{Z}/_{R_m}$ se definen de manera sencilla las operaciones de suma y multiplicación. A partir de este punto es necesario poseer conocimientos básicos de Álgebra Moderna.

DEFINICIÓN 3.2.5 $\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}.$

De esta definición se deduce:

TEOREMA 3.2.4

El conjunto de las clases de restos $\mathbb{Z}/_{R_m}$ constituye con las operaciones definidas anteriormente un anillo conmutativo.

La demostración queda como ejercicio. Se debe demostrar que las operaciones suma y producto están bien definidas, que $(\mathbb{Z}/_{R_m}, +)$ es un grupo abeliano y que el producto es conmutativo y distributivo respecto a la suma y tiene elemento neutro $\overline{1}$.

TEOREMA 3.2.5

$\mathbb{Z}/_{R_m}$ tiene divisores del cero para m compuesto. Si $m = p$ es primo, entonces $\mathbb{Z}/_{R_p}$ es un cuerpo de característica p.

Demostración:

- Sea $m = m_1 m_2$ con $0 < m_i < m$. Entonces $\overline{m_i} \neq \overline{0}$ para $i = 1, 2$. Pero

  $$\overline{m_1} \cdot \overline{m_2} = \overline{m_1 \cdot m_2} = \overline{0},$$

  por lo que $\mathbb{Z}/_{R_m}$ tiene divisores del cero.

- Sea $m = p$ primo. Si $\overline{a}\overline{b} = \overline{0}$ en $\mathbb{Z}/_{R_p}$, entonces $p|ab$, por lo que $p|a$ o $p|b$. Luego $\overline{a} = \overline{0}$ ó $\overline{b} = \overline{0}$, por lo que $\mathbb{Z}/_{R_p}$ no tiene divisores del cero, lo que lo hace ser un cuerpo.

  Pero para todo $\overline{a} \in \mathbb{Z}/_{R_p}$ se tiene

  $$p\overline{a} = \overline{pa} = \overline{0},$$

  siendo así $\mathbb{Z}/_{R_p}$ un cuerpo de característica p. **Q.e.d.**

Surge la pregunta ¿Es posible dividir ambos miembros de una congruencia por un entero b?

EJEMPLO: $14 \equiv 8(mod\ 6)$. Si fuera posible cancelar sería $7 \equiv 4(mod\ 6)$, lo cual es falso.

Sin embargo, se cumple el siguiente teorema.

TEOREMA 3.2.6

Sean a, b, c, m números enteros $(m > 0)$ tales que $ac \equiv bc(mod\ m)$. Sea además $d = (c, m)$. Entonces es $a \equiv b(mod\ \frac{m}{d})$.

Demostración: Como $ac \equiv bc(mod\ m)$, entonces $m|(ac - bc) = c(a - b)$. De aquí que existe un entero k tal que $c(a - b) = km$. Dividiendo esta última ecuación por d se obtiene.

$$\frac{c(a-b)}{d} = \frac{km}{d}.$$

Pero $d = (c, m)$, es decir $\frac{m}{d} \in \mathbb{Z}$ y $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$, y por lo tanto $\frac{m}{d}$ divide a $(a - b)$, de donde se obtiene la tesis del teorema. **Q.e.d.**

EJEMPLO: $14 \equiv 8(mod\ 6)$ y $(2, 6) = 2$, entonces es $7 \equiv 4(mod\ \frac{6}{2})$. Es decir, $7 \equiv 4(mod\ 3)$.

COROLARIO 3.2.1

Si $(c, m) = 1$ y $ac \equiv bc(mod\ m)$, entonces es $a \equiv b(mod\ m)$.

Demostración: Utilizando $d = 1$ en el teorema 3.2.6. **Q.e.d.**

EJEMPLO: $42 \equiv 7(mod\ 5)$ y $(5, 7) = 1$, entonces es $6 \equiv 1(mod\ 5)$.

TEOREMA 3.2.7

Si a, b, c, d, m son números enteros $(m > 0)$ tales que

$$a \equiv b(mod\ m) \quad y \quad c \equiv d(mod\ m),$$

entonces es

i) $a \pm c \equiv b \pm d(mod\ m)$.

ii) $ac \equiv bd(mod\ m)$.

Demostración: En este caso se tiene que $m|(a - b)$ y $m|(c - d)$. Entonces se cumple que $m|((a \pm c) - (b \pm d))$, de donde se deduce i).

Por otra parte es $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$. De aquí que $m|(ac - bd)$, de donde se deduce ii). **Q.e.d.**

EJEMPLO: $13 \equiv 3(mod\ 5)$ y $7 \equiv 2(mod\ 5)$, entonces es $20 \equiv 5(mod\ 5)$, $6 \equiv 1(mod\ 5)$ y $91 \equiv 6(mod\ 5)$.

TEOREMA 3.2.8

Si $\{r_1, r_2, \ldots, r_m\}$ es un sistema completo de restos módulo m, $b \in \mathbb{Z}$ y a es un entero positivo primo relativo con m, entonces $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ es también un sistema completo de restos módulo m.

Demostración: Supongamos que existen índices enteros $1 \leq j, k \leq m$ tales que

$$ar_j + b \equiv ar_k + b(mod\ m).$$

Entonces m divide a $(ar_j + b) - (ar_k + b) = a(r_j - r_k)$. Pero como $(a, m) = 1$, entonces m divide a $(r_j - r_k)$, de donde se deduce que $r_j \equiv r_k(mod\ m)$. Pero esto último es imposible por ser $\{r_1, r_2, \ldots, r_m\}$ un sistema completo de restos módulo m. Entonces el sistema $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ es un sistema de m números incongruentes módulo m, de donde se deduce la tesis del teorema. **Q.e.d.**

TEOREMA 3.2.9 *Si $a \equiv b(mod\ m)$, entonces $a^k \equiv b^k(mod\ m)$ para todo $k > 0$.*

Demostración: Como $a \equiv b(mod\ m)$, entonces $m|(a - b)$. Pero

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1}).$$

Entonces $(a - b)$ divide a $(a^k - b^k)$ y por ello m divide también a $(a^k - b^k)$, de donde se deduce la tesis del teorema. **Q.e.d.**

TEOREMA 3.2.10

Si $m_1, m_2, ..., m_k$ son enteros positivos tales que $a \equiv b(mod\ m_i)$, entonces es $a \equiv b(mod\ [m_1, m_2, ..., m_k])$.

Demostración: Se deduce del hecho de que $[m_1, m_2, ..., m_k]$ divide a $(a - b)$. **Q.e.d.**

Las congruencias resultan de gran utilidad para encontrar criterios de divisibilidad.

EJEMPLO: Encontrar un criterio de divisibilidad por 3.

Para ello se escribe el número entero n en notación decimal

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0.$$

Se desea que 3 divida a n, entonces debe ser $n \equiv 0(mod\ 3)$, es decir

$$a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0 \equiv 0(mod\ 3).$$

Pero $10 \equiv 1(mod\ 3)$, entonces es

$$a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0 \equiv a_m + a_{m-1} + \ldots + a_1 + a_0 \equiv 0(mod\ 3).$$

De ello se deduce que

Un entero n es divisible por 3, si la suma de sus cifras es divisible por 3.

3.3. Congruencias lineales

En cuanto a las congruencias lineales $ax \equiv b(mod\ m)$ se cumple:

TEOREMA 3.3.1

La congruencia $ax \equiv b(mod\ m)$ tiene solución si y sólo si $(a,m)|b$. En ese caso existen exactamente (a,m) soluciones incongruentes módulo m.

Demostración:

(Necesidad) Si existe x tal que $ax \equiv b(mod\ m)$, entonces $ax = b + km$ para algún entero k, es decir, $ax + km = b$. Pero $(a,m)|(ax - km)$, por lo que $(a,m)|b$.

(Suficiencia) Sea $(a,m) = d$ y $d|b$. Aquí se dan dos casos, a saber, $d = 1$ ó $d > 1$.

- Si $d = 1$, por el teorema 2.1.5 existen $u, v \in \mathbb{Z}$ con $au + mv = 1$ y multiplicando por b se deduce que existen $x, y \in \mathbb{Z}$ con $ax + my = b$. Así es $ax \equiv b(mod\ m)$.

  Para la unicidad sean x, x' con

  $$ax \equiv b(mod\ m), \qquad ax' \equiv b(mod\ m).$$

  Entonces es $a(x - x') \equiv 0(mod\ m)$, es decir, $a(x - x') = km$ para cierto entero k. Como $d = 1$, se tiene que $x - x' = k'm$ para cierto entero k', de donde $x \equiv x'(mod\ m)$.

- Si $d > 1$, como $d|b$, se hace

  $$a = a'd, \qquad b = b'd, \qquad m = m'd.$$

  Aquí se tiene

  $$\begin{aligned} ax \equiv b(mod\ m) \quad &\Rightarrow \quad ax = b + km \quad \Rightarrow \quad a'dx = b'd + km'd \\ &\Rightarrow \quad a'x \equiv b'(mod\ m') \quad \text{con} \quad (a', m') = 1. \end{aligned}$$

  Así se cae en el caso anterior, que ya ha sido demostrado.

Finalmente, de haber solución existe la clase solución $x \equiv x_0(mod\ m)$, de donde se deduce la existencia de las m soluciones incongruentes módulo m

$$x \equiv x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'(mod\ m).$$

Q.e.d.

La demostración del teorema indica una vía de resolución de tales ecuaciones. A continuación se muestran dos ejemplos:

EJEMPLOS:

1. La congruencia $7x \equiv 1(mod\ 31)$ tiene solución única, pues $(7, 31) = 1|1$.

   Esta congruencia es equivalente a la ecuación diofántica $7x = 31y + 1$. Al aplicar el algoritmo de Euclides para expresar a $(7, 31) = 1$ como combinación lineal de 7 y 31 se obtiene

   $$1 = 7(7) - 2(31).$$

   De aquí que $x_0 \equiv 7(mod\ 31)$ es la solución única de la congruencia lineal.

2. La congruencia $3x \equiv 6(mod\ 27)$ tiene tres soluciones incongruentes módulo 27, pues $(3, 3127) = 3|6$.

   Por la ley de cancelación se obtiene la congruencia $x \equiv 2(mod\ 9)$, equivalente a la inicial, de la cual se deduce la primera solución

   $$x_0 \equiv 2(mod\ 27),$$

   y de ellas

   $$x_0 + 9 \equiv 11(mod\ 27) \quad \text{y} \quad x_0 + 2 \cdot 9 \equiv 20(mod\ 27).$$

Las congruencias también pueden ser resueltas de modo muy similar a como se resuelven las ecuaciones lineales en números reales. Por ejemplo, la ecuación $2x = 3$ se resuelve multiplicándola por el inverso de 2 (es decir $\frac{1}{2}$). Así se tiene $x = 3(\frac{1}{2}) = \frac{3}{2}$.

Para aplicar éste método a las congruencias habrá que definir el concepto de inverso.

Definición 3.3.1

Si a es un número entero tal que $(a, m) = 1$, entonces la solución de la congruencia $ax \equiv 1(mod\ m)$ se llama ***inverso de a módulo m*** *y se denota $\bar{a}$.*

Nótese que si $(a, m) = 1$, la ecuación $ax \equiv 1(mod\ m)$ sólo tiene una solución incongruente módulo m. Es decir, ella tiene infinitas soluciones, pero todas son congruentes módulo m entre sí.

EJEMPLO: Hallar el inverso módulo 31 de 7.

$$7x \equiv 1(mod\ 31).$$

Es obvio que $(7, 31) = 1$. De modo que al resolver la ecuación diofántica $7x - 31y = 1$ se obtiene $x = 9$ y por ello la solución de la congruencia es $x \equiv 9(mod\ 31)$. De aquí

que finalmente 9 es el inverso de 7 módulo 31.

Conociendo el inverso módulo m de a, se resuelve entonces fácilmente la congruencia lineal. Si $\bar{a}$ es el inverso módulo m de a, entonces es $\bar{a}a \equiv 1(mod\ m)$, de donde se deduce que $ax \equiv b(mod\ m)$ y al multiplicar por $\bar{a}$ se obtiene $\bar{a}ax \equiv \bar{a}b(mod\ m)$. Pero $\bar{a}a \equiv 1(mod\ m)$, de donde finalmente es

$$x \equiv \bar{a}b(mod\ m).$$

EJEMPLO: Ya se ha visto que la ecuación $7x \equiv 22(mod\ 31)$ tiene solución única (como clase), pues $(7, 31) = 1$, y se conoce además que $\bar{7} = 9$, es decir $7 \cdot 9 \equiv 1(mod\ 31)$. Al multiplicar entonces la congruencia por 9 es

$$9 \cdot 7x \equiv x \equiv (9)22 \equiv 198 \equiv 12(mod\ 31)$$

Es decir, la solución buscada es

$$x \equiv 12(mod\ 31).$$

EJEMPLO: Veamos ahora otro ejemplo.

$$7x \equiv 4(mod\ 12).$$

Como $(7, 12) = 1$, entonces 7 tiene inverso módulo 12. Este se calcula solucionando la ecuación $7x \equiv 1(mod\ 12)$, de donde se obtiene $\bar{7} = -5$. Entonces

$$\begin{aligned} 7x &\equiv 4(mod\ 12) \\ (-5)7x &\equiv x \equiv (-5)4 \equiv -20 \equiv 4(mod\ 12), \end{aligned}$$

de donde

$$S = \{x \in \mathbb{Z} : x \equiv 4(mod\ 12)\}.$$

En el caso de los números reales los únicos números que son sus propios inversos son 1 y -1. Aquí sucede algo similar:

Teorema 3.3.2

Sea p un número primo y a un número entero cualquiera. Entonces a es su propio inverso módulo p si y sólo si $a \equiv \pm 1(mod\ p)$.

Demostración:

(Necesidad:) Sea a su propio inverso módulo p. Entonces es $aa = a^2 \equiv 1(mod\ p)$ y por ello p divide a $a^2 - 1 = (a-1)(a+1)$. Pero p es primo, por lo que p divide a $(a-1)$ o p divide a $(a+1)$, de donde se deduce que $a \equiv 1(mod\, p)$ o $a \equiv -1(mod\, p)$.

(Suficiencia:) Sea ahora $a \equiv \pm 1(mod\ p)$, entonces $aa = a^2 \equiv 1(mod\ p)$, lo cual implica que a es su propio inverso módulo p. **Q.e.d.**

3.3.1. Ejercicios

1. Determine si es verdadero (V) o falso (F):
   a) $13 \equiv 1(mod\ 2)$ b) $111 \equiv -9(mod\ 40)$
   c) $-3 \equiv 30(mod\ 11)$ d) $69 \equiv 62(mod\ 7)$

2. Demuestre si a es un número entero, entonces es
$$a^2 \equiv \begin{cases} 0(mod\ 4) & \text{si } a \text{ es par} \\ 1(mod\ 4) & \text{si } a \text{ es impar} \end{cases}$$

3. Demuestre si a es un entero impar, entonces $a^2 \equiv 1(mod\ 8)$.

4. Halle el menor residuo no negativo módulo 13 de
   a) 22 b)100 c) -1 d) -100

5. Demuestre que si a, b, m, n son números enteros $(m > 0, n > 0)$ tales que n divide a m y $a \equiv b(mod\ m)$, entonces $a \equiv b(mod\ n)$.

6. Demuestre que si $n > 0$ es un número impar, entonces es
$$1 + 2 + ... + (n-1) \equiv 0(mod\ n).$$

7. Demuestre que para todo entero positivo n se cumple que
   $4^n \equiv 1 + 3n(mod\ 9)$.

8. Halle un sistema completo de restos módulo 13 compuesto únicamente de números impares.

9. Halle el menor resto positivo de los siguientes números según el módulo indicado
   a) $6_{mod\ 7}$ b) $12_{mod\ 13}$.

10. Determine criterios de divisibilidad
    a) por 9 b) por 11.

11. Solucione
    a) $2x \equiv 5(mod\ 7)$ b) $3x \equiv 6(mod\ 9)$
    c) $103x \equiv 444(mod\ 999)$ d) $128x \equiv 833\ (mod\ 101)$
    e) $17x \equiv 14(mod\ 21)$ f) $6789783x \equiv 2474010(mod\ 28927591)$
    ¿En cuáles casos se puede utilizar la técnica del inverso?

12. Sean a, b, m enteros con $m > 0$ y $(a, m) = 1$. Los siguientes dos incisos proponen un método para solucionar la congruencia lineal $ax \equiv b(mod\ m)$

a) Demuestre que si x es solución de la congruencia $ax \equiv b(mod\ m)$, entonces x es también solución de $a_1 x \equiv -b\left[\frac{m}{a}\right]\ (mod\ m)$, siendo a_1 el menor residuo positivo de m módulo a. (Note que esta congruencia es del mismo tipo que la original con un coeficiente de la incógnita x positivo y menor)

b) Iterando el paso *a)* se obtiene una sucesión de congruencias módulo m con coeficientes $a_0 = a > a_1 > a_2 > a_3 > \ldots$. Demuestre que existe un entero positivo n tal que $a_n = 1$, de modo que en el enésimo paso se obtiene la congruencia lineal $x \equiv B(mod\ m)$.

c) Calcule por este método $6x \equiv 7(mod\ 23)$.

d) Elabore un programa de computación que implemente este método.

13. ¿Para qué valores enteros de c con $0 \leq c < 30$ tiene solución la congruencia $12x \equiv c(mod\ 30)$? ¿Cuántas soluciones incongruentes tiene?

14. Encuentre el inverso módulo m de a si:
    a) $a = 2,\ m = 13$ b) $a = 5,\ m = 13$
    c) $a = 4,\ m = 17$ d) $a = 16,\ m = 17$.

15. Sean $\bar{a}$ y $\bar{b}$ inversos módulo m de a y b respectivamente. Demuestre que $\bar{a}\bar{b}$ es el inverso módulo m de ab.

16. Sea la congruencia lineal en dos variables $ax + by \equiv c(mod\ m)$ y sea además $d = (a, b, m)$.

    a) Demuestre que existe solución si y sólo si d divide a c.

    b) Haciendo $dz = ax + by$, demuestre que si d divide a c entonces hay dm soluciones incongruentes.

    c) Solucione la ecuación $2x + 3y. \equiv 1(mod\ 7)$.

17. Sea p un número primo impar y k un entero positivo. Demuestre que la congruencia $x^2 \equiv 1(mod\ p^k)$ tiene exactamente dos soluciones incongruentes que son $x \equiv \pm 1(mod\ p^k)$.

3.4. La clase prima de restos

Definición 3.4.1

La clase de restos $\overline{a}$ se llama ***clase prima de restos módulo*** *m si $(a, m) = 1$.*

Selecionando un representante de cada una de estas clases se obtiene un sistema reducido de restos módulo m, como se expresa en la definición siguiente.

DEFINICIÓN 3.4.2

Se conoce como ***sistema reducido de restos módulo*** m *enteros a cualquier conjunto maximal* $\{a_1, a_2, \ldots, a_k\}$ *de enteros primos relativos con* M *que sean incongruentes módulo* m *dos a dos; es decir, tal que para todos* $i \neq j$ *se cumple* $a_i \not\equiv a_j (mod\ m)$ *y* $(a_i, m) = 1$.

TEOREMA 3.4.1

Las clases primas de restos módulo m *constituyen un grupo multiplicativo abeliano, que se conoce como* ***grupo de las clases primas de restos módulo*** m *o* ***grupo del sistema reducido de restos módulo*** m.

Demostración: Sea G el conjunto de las clases primas de restos módulo m.

1. $\overline{a}, \overline{b} \in G \quad \Rightarrow \quad (a, m) = 1 = (b, m)$. Así es $(ab, m) = 1$, por lo que se cumple que $\overline{a} \cdot \overline{b} = \overline{ab} \in G$
2. La asociatividad y conmutatividad se deducen de lo ya conocido.
3. La unidad es $\overline{1}$.
4. Del teorema 3.3.1 se deduce la existencia del inverso único. **Q.e.d.**

Una de la más aplicadas funciones aritméticas se debe a Leonard Euler.

DEFINICIÓN 3.4.3

La función aritmética (en enteros) ϕ ***de Euler*** *se define como*

$\phi(m) =$ *número de las clases primas de restos módulo* m.

NOTA: $\phi(m)$ es el número de enteros positivos menores que m, que son primos relativos con m. Por ejemplo,

$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(4) = 2, \quad \phi(5) = 4, \quad \phi(6) = 2.$$

Si p es primo, entonces obviamente es $\phi(p) = p - 1$.

TEOREMA 3.4.2 $\displaystyle\sum_{d|n} \phi(d) = n.$

Demostración: Sea $\phi_d(n)$ la cantidad de números naturales $x \leq n$ con $(x, n) = d$. Entonces

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

Hacemos $x = x'd$ y $n = n'd$. Entonces es $(x', n') = 1$, de donde $\phi_d(n) = \phi(n')$ y

$$n = \sum_{d|n} \phi_d(n) = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{t|n} \phi(t) \qquad \textbf{Q.e.d.}$$

Sea $n = p^\alpha$ una potencia de primo. Aplicando el teorema se tiene que

$$\begin{aligned} \phi(1) + \phi(p) + \ldots + \phi(p^{\alpha-1}) + \phi(p^\alpha) &= p^\alpha \\ \phi(1) + \phi(p) + \ldots + \phi(p^{\alpha-1}) &= p^{\alpha-1}. \end{aligned}$$

De la resta de ambas igualdades se obtiene

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right).$$

DEFINICIÓN 3.4.4

Una función aritmética f (en enteros) se dice ***multiplicativa*** *si $(m, n) = 1$ implica que $f(mn) = f(m)f(n)$.*

Se comprobará que la función de Euler es multiplicativa, con lo cual se podrá calcular su valor en todo entero positivo. Para ello conviene considerar el siguiente ejemplo.

EJEMPLO: Sea $n = 4$ y $m = 9$, de modo que $(n, m) = 1$ y $nm = 36$. Escribimos ordenadamente en columnas los números de 1 a 36 en un arreglo de 4×9.

1	5	9	13	17	21	25	29	33
2	6	10	14	18	22	26	30	34
3	7	11	15	19	23	27	31	35
4	8	12	16	20	24	28	32	36

A fin de determinar los números primos relativos con 36 se tachan primeramente todos los números pares (columnas 2 y 4) con lo cual quedan por analizar $2 = \varphi(4)$ columnas. En las columnas restantes se tachan entonces todos los números que son primos relativos con 9; es decir, quedan $6 = \varphi(9)$ números sin tachar (en rojo) en esas columnas, que son los números primos relativos con 36.

1	5	9	13	17	21	25	29	33
2	6	10	14	18	22	26	30	34
3	7	11	15	19	23	27	31	35
4	8	12	16	20	24	28	32	36

Se ha comprobado así que $\varphi(4 \cdot 9) = \varphi(4)\varphi(9)$. A continuación se generaliza este resultado.

LEMA 3.4.1

Sean los números naturales m, m' con $(m, m') = 1$. Si a y a' recorren respectivamente sistemas completos de restos módulos m y m', entonces $a'm + am'$ recorre un sistema completo de restos módulo mm'.

Demostración: Está claro que existen mm' números de la forma $a'm + am'$. Sea

$$a'_1 m + a_1 m' \equiv a'_2 m + a_2 m' (mod\ mm').$$

Entonces, al plantear la igualdad correspondiente y despejar en m y en m', se obtiene

$$\begin{aligned} a_1 m' &\equiv a_2 m' (mod\ m) \\ a'_1 m &\equiv a'_2 m (mod\ m'). \end{aligned}$$

Como $(m, m') = 1$, se deduce que

$$\begin{aligned} a_1 &\equiv a_2 (mod\ m) \\ a'_1 &\equiv a'_2 (mod\ m'), \end{aligned}$$

lo que contradice la hipótesis de que a y a' recorren respectivamente sistemas completos de restos módulos m y m'. Así, los números de la forma $a'm + am'$ son incongruentes módulo mm' entre sí. **Q.e.d.**

TEOREMA 3.4.3

$$(m, m') = 1 \qquad \Rightarrow \qquad \phi(mm') = \phi(m)\phi(m').$$

Ello indica que la función ϕ de Euler es multiplicativa.

Demostración: Supongamos que a y a' recorren respectivamente sistemas completos de restos módulos m y m'. Por el lema anterior $a'm + am'$ recorre un sistema completo de restos módulo mm'. Aquí se tiene

$$\begin{aligned} (a'm + am', mm') = 1 \quad &\Leftrightarrow \quad (a'm + am', m) = 1 \ \text{ y } \ (a'm + am', m') = 1 \\ &\Leftrightarrow \quad (am', m) = 1 \ \text{ y } \ (a'm, m') = 1 \\ &\Leftrightarrow \quad (a, m) = 1 \ \text{ y } \ (a', m') = 1. \end{aligned}$$

Entonces $a'm + am'$ es primo relativo con mm' si y sólo si a es primo relativo con m y a' es primo relativo con m'. De aquí que $\phi(mm') = \phi(m)\phi(m')$. **Q.e.d.**

Llegados a este punto, ya se puede presentar la fórmula general.

TEOREMA 3.4.4

Si p denota a los divisores primos de m, entonces es

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

Demostración: Sea

$$m = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad \text{con} \quad p_i \neq p_j \quad \text{para} \quad i \neq j.$$

Ya se conoce que

$$\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right).$$

Por el teorema anterior es entonces

$$\phi(m) = \prod_{i=1}^{r} \phi\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Q.e.d.

Uno de los más importantes resultados de Fermat es el que plantea: Si p es primo y a es cualquier entero no divisible por p, entonces p divide a $a^{p-1} - 1$. Fermat comunicó el resultado a Frenicle de Besy[1] en una carta fechada el 18 de octubre de 1640, sólamente con el comentario

"*yo enviaría la demostración, si no temiera que será demasiado larga*".

Desde entonces este teorema se conoce como "Pequeño Teorema de Fermat" para distinguirlo del "Gran o Último Teorema". Casi 100 años transcurrieron hasta que Euler publicó la primera demostración del Pequeño Teorema en 1736.

TEOREMA 3.4.5 ***Pequeño Teorema de Fermat***

Sea a un número entero positivo y p un número primo que no lo divide, entonces es

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

Demostración: La esencia de esta demostración consiste en reconocer que

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

Para ello se consideran los enteros $a, 2a, 3a, ..., (p-1)a$. Si p dividiera a ja, siendo j positivo menor que p, entonces p tendría que dividir a a (pues p es primo y no divide

[1] Bernard Frenicle de Bessy (1605-1670)

a j), lo cual constituye una contradicción. Entonces p no divide a ja para todo j entero positivo menor que p.

Por otro lado, si fuera $ja \equiv ka(mod\ p)$ con j, k enteros positivos menores que p, entonces sería $j \equiv k(mod\ p)$, pues $(a, p) = 1$, lo cual también resultaría contradictorio. Entonces el conjunto $\{a, 2a, 3a, \ldots, (p-1)a\}$ es un sistema completo de restos módulo p, el cual es congruente (reordenándolo en caso necesario) al sistema $\{1, 2, 3, \ldots p-1\}$. De ello se deduce que

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)(mod\ p).$$

Es decir,

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

Pero $((p-1)!, p) = 1$, por lo que

$$a^{p-1} \equiv 1(\quad \text{mód } p).$$

Q.e.d.

Más adelante Euler generaliza el resultado.

TEOREMA 3.4.6 ***Euler-Fermat***

$$(a, m) = 1 \qquad \Rightarrow \qquad a^{\phi(m)} \equiv 1(mod\ m).$$

Demostración: (Esta demostración se desarrollará utilizando las clases primas de restos, para que el lector observe la semejanza con el método utilizado en el teorema anterior). Sea

$$G = \{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{\phi(m)}}\}$$

el grupo de las clases primas de restos módulo m. Si $\overline{a} \in G$, entonces

$$G = \{\overline{aa_1}, \overline{aa_2}, \ldots, \overline{aa_{\phi(m)}}\}$$

es nuevamente el grupo completo de las clases primas de restos módulo m. De aquí que

$$\overline{aa_1} \cdot \overline{aa_2} \cdots \overline{aa_{\phi(m)}} = \overline{a_1} \cdot \overline{a_2} \cdots \overline{a_{\phi(m)}} \qquad \Rightarrow \qquad \overline{a^{\phi(m)}} = \overline{1},$$

por lo que $a^{\phi(m)} \equiv 1(mod\ m)$. **Q.e.d.**

NOTA: En general $\phi(m)$ no es el menor exponente α para el cual se cumple que $a^{\alpha} \equiv 1(mod\ m)$. Por ejemplo, $2^3 \equiv 1(mod\ 7)$ y $\phi(7) = 6$.

Sin embargo, si d es el menor exponente para el cual se cumple que $a^d \equiv 1(mod\ m)$ con $(a, m) = 1$, entonces $d|\phi(m)$. Para comprobarlo, sea

$$\phi(m) = kd + r \quad \text{con} \qquad 0 \leq r < d.$$

Se tiene que

$$1 \equiv a^{\phi(m)} \equiv a^{kd+r} \equiv (a^d)^k a^r \equiv a^r (mod\ m),$$

pues $a^d \equiv 1(mod\ m)$ y d es minimal. Entonces tiene que ser $r = 0$, y por tanto $a^d \equiv 1(mod\ m)$.

La función ϕ de Euler también brinda una **técnica para solucionar la congruencia lineal** $ax \equiv b(mod\ m)$ con $(a, m) = 1$. Pues como $a^{\phi(m)} \equiv 1(mod\ m)$, entonces

$$ax \equiv ba^{\phi(m)}(mod\ m),$$

de donde

$$x \equiv ba^{\phi(m)-1}(mod\ m).$$

Es claro que esta técnica es más teórica que práctica, pues $a^{\phi(m)}$ puede resultar muy difícil de calcular.

TEOREMA 3.4.7 ***Wilson***

Para todo número primo p se cumple

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

Demostración: Si $p = 2$ es obvio que $1! \equiv -1(mod\ 2)$. Para $p > 2$, sea el grupo de las clases primas de restos

$$G = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

En G la ecuación $\overline{a} \cdot \overline{x} = \overline{1}$ tiene solución única. Veamos cuándo es $\overline{x} = \overline{a}$.

$$\begin{array}{lllll} \overline{a^2} = \overline{1} & \Leftrightarrow & a^2 \equiv 1(mod\ p) & \Leftrightarrow & (a-1)(a+1) \equiv 0(mod\ p) \\ & \Leftrightarrow & \overline{a} = \overline{1} \quad \vee & \overline{a} = \overline{p-1}. & \end{array}$$

Entonces es

$$\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdots \overline{p-1}.$$

Y agrupando las clases con $\overline{a} \cdot \overline{b} = \overline{1}$ se obtiene

$$\overline{(p-1)!} = \overline{p-1},$$

lo que demuestra el teorema. **Q.e.d.**

NOTA: El teorema de Wilson[2] constituye un criterio para determinar si un número es primo, pues su recíproco también es válido. Es decir

[2]John Wilson (1741-1793)

Si $(n-1)! \equiv -1(mod\ n)$ para $n > 1$, entonces $n = p$ es un número primo.

Demostración: Supongamos que n es compuesto, es decir, existe d que divide a n con $1 < d < n$. Entonces $d|(n-1)!$. Pero $(n-1)! \equiv -1(mod\ n)$ implica que $(n-1)! = kn-1$, de donde se deduce que $d|-1$, lo cual constituye una contradicción. **Q.e.d.**

3.5. Las ecuaciones diofánticas lineales desde las congruencias

Considere ahora nuevamente las ecuaciones en $x_1, \ldots, x_n \in \mathbb{Z}$

$$a_1x_1 + \ldots + a_nx_n = c$$

con $a_1, \ldots, a_n, c \in \mathbb{Z}$, desde la visión de las congruencias. Para ello se analiza primeramente el caso

$$ax + by = c \tag{3.1}$$

con $a, b, c \in \mathbb{Z}$ y $a, b \neq 0$.

Nótese que esa ecuación representa una recta en el plano euclidiano. Si se llama **nodo** al punto $P(x, y)$ si $x, y \in \mathbb{Z}$, entonces desde el punto de vista geométrico se trata de determinar si sobre la recta de ecuación 3.1 aparecen nodos.

Es claro que para que la ecuación tenga solución es necesario que $(a, b)|c$. Para simplificar el análisis nos limitaremos al caso $(a, b) = 1$. Analicemos la ecuación (3.1) módulo $|b|$, es decir,

$$ax + by \equiv c(mod\ |b|).$$

De esta ecuación se tiene

$$ax \equiv c(mod\ |b|),$$

y como $(a, b) = 1$, se sabe que la solución está dada por

$$x \equiv ca^{\phi(|b|)-1}(mod\ |b|),$$

es decir,

$$x = ca^{\phi(|b|)-1} + kb.$$

Al sustituir en (3.1) se tiene

$$a\left(ca^{\phi(|b|)-1} + kb\right) + by = c,$$

de donde, despejando, se obtiene

$$y = c\frac{1 - a^{\phi(|b|)}}{b} - ka,$$

que es entero por el teorema de Fermat-Euler.

Sea ahora la ecuación

$$a_1x_1 + \ldots + a_nx_n = c, \qquad a_1, \ldots, a_n, c \in \mathbb{Z}.$$

Para solucionarla se reduce a una ecuación con $n-1$ incógnitas.

Sea $d_k = (a_1, \ldots, a_k)$ para $k = 2, 3, \ldots, n$ y sea $d_n = 1$. Entonces la ecuación

$$a_1x_1 + \ldots + a_{n-1}x_{n-1} = c - a_nx_n$$

implica obviamente que

$$a_nx_n \equiv c(mod\ d_{n-1}),$$

que tiene solución única por ser $(a_n, d_{n-1}) = d_n = 1$. Así es

$$x_n = ca^{\phi(d_{n-1})} + kd_{n-1}.$$

Al sustituir en la ecuación original se obtiene la ecuacón con $n-1$ incógnitas

$$a_1x_1 + \ldots + a_{n-1}x_{n-1} = c\left(1 - a^{\phi(d_{n-1})}\right) - kd_{n-1}.$$

3.6. Congruencias lineales simultáneas

A continuación se estudian dos tipos de sistemas de congruencias lineales.

3.6.1. Sistemas en una variable con diferentes módulos

Un famoso teorema ofrece la solución de los sistemas de congruencias lineales con diferentes módulos.

TEOREMA 3.6.1 ***Teorema Chino del Resto***

Sean $m_1, \ldots, m_n$ enteros positivos primos relativos dos a dos. Entonces el sistema $x \equiv a_k(mod\ m_k)$ $(k = 1, ..., n)$ tiene solución única módulo $M = m_1m_2 \ldots m_n$.

Demostración:

i) (Existencia) Se construye primero una solución. Sea

$$M_k = \frac{M}{m_k} = \frac{m_1 m_2 \dots m_n}{m_k} = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_n.$$

Se sabe que $(M_k, m_k) = 1$, pues $(m_i, m_k) = 1$ para todo $i \neq k$. Entonces existe el inverso módulo m_k de M_k. Sea éste igual a y_k, o sea $M_k y_k \equiv 1(mod\ m_k)$. Sea ahora $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$. Para cada m_k fijo se tiene que m_k divide a M_i para todo $i \neq k$, por lo que es

$$M_i \equiv 0(mod\ m_k) \quad \forall i \neq k.$$

Entonces se tiene

$$x \equiv a_k M_k y_k (mod\ m_k).$$

Pero $M_k y_k \equiv 1(mod\ m_k)$, entonces es

$$x \equiv a_k (mod\ m_k),$$

por lo que x es una solución del sistema dado.

ii) Unicidad. Para comprobar que cualesquiera dos soluciones son congruentes módulo m, sean x_0, x_1 soluciones. Entonces $x_0 \equiv x_1 \equiv a_k (mod\ m_k)$ para todo $k = 1, ..., n$. De ahí que m_k y por tanto M divide a $(x_0 - x_1)$, concluyendo así que

$$x_0 \equiv x_1 (mod\ M).$$

Q.e.d.

EJEMPLO:

$$\begin{cases} x \equiv 1(mod\ 3) \\ x \equiv 2(mod\ 5) \\ x \equiv 3(mod\ 7) \end{cases}$$

Aquí es

$$M = 3 \cdot 5 \cdot 7 = 105,$$

de donde

$$\begin{aligned} M_1 &= \frac{105}{3} = 35, \\ M_2 &= \frac{105}{5} = 21, \\ M_3 &= \frac{105}{7} = 15. \end{aligned}$$

Así

$$\begin{array}{rcll} 35y_1 \equiv 1(mod\ 3) & \Longrightarrow & 2y_1 \equiv 1(mod\ 3) & \Longrightarrow \quad y_1 \equiv 2(mod\ 3), \\ 21y_2 \equiv 1(mod\ 5) & \Longrightarrow & y_2 \equiv 1(mod\ 5), & \\ 5y_3 \equiv 1(mod\ 7) & \Longrightarrow & y_3 \equiv 1(mod\ 7). & \end{array}$$

Luego,

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 157 \equiv 52(mod\ 105)$$

de donde

$$x \equiv 52(mod\ 105).$$

Este tipo de sistemas también puede ser resuelto utilizando ecuaciones diofánticas lineales. En el ejemplo siguiente se muestra cómo hacerlo.

EJEMPLO:

$$\begin{cases} x \equiv 1(mod\ 5) \\ x \equiv 2(mod\ 6) \\ x \equiv 3(mod\ 7) \end{cases}.$$

La primera ecuación del sistema es $x \equiv 1(mod\ 5)$, de donde se obtiene

$$x = 5t + 1.$$

La segunda ecuación es $x \equiv 2(mod\ 6)$. Se sustituye el valor obtenido de x para obtener

$$5t + 1 \equiv 2(mod\ 6),$$

siendo así $t \equiv -1 \equiv 5(mod\ 6)$. Entonces es $t = 6u + 5$.

Por último, la tercera ecuación es $x \equiv 3(mod\ 7)$. Al sustituir los valores de x, t es

$$x = 5t + 1 = 5(6u + 5) + 1 = 30u + 26 \equiv 3(mod\ 7).$$

Es decir,

$$30u \equiv -23 \equiv 5(mod\ 7),$$

de donde se obtiene

$$u \equiv -15 \equiv 6(mod\ 7).$$

De aquí se deduce que $u = 7v + 6$. Sustituyendo ahora de vuelta en el valor de x se obtiene

$$x = 30u + 26 = 30(7v + 6) + 26 = 210v + 206.$$

Y por tanto la solución del sistema es

$$x \equiv 206(mod\ 210).$$

3.6.2. Ejercicios

1. Solucione los sistemas de congruencias lineales siguientes:

   a) $\begin{cases} x = 1(mod\ 2) \\ x = 2(mod\ 3) \end{cases}$ b) $\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 1(mod\ 5) \\ x \equiv 0(mod\ 3) \end{cases}$

   c) $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 2(mod\ 5) \\ x \equiv 0(mod\ 4) \end{cases}$ d) $\begin{cases} x \equiv 4(mod\ 11) \\ x \equiv 3(mod\ 17) \end{cases}$

   e) $\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \end{cases}$ f) $\begin{cases} x \equiv 0(mod\ 2) \\ x \equiv 0(mod\ 3) \\ x \equiv 1(mod\ 5) \\ x \equiv 6(mod\ 7) \end{cases}$

2. Un grupo de 17 monos agrupan sus bananas en 11 pilas iguales quedando 6 bananas afuera. Al dividir sus bananas en 17 grupos iguales no sobra ninguna. ¿Cuál es el menor número posible de bananas?

3. Los tres niños de una familia tienen sendos muñecos, cuyos pies tienen longitud de $5, 7$ y 11 centímetros respectivamente. Al medir el largo del comedor de su casa con los pies de sus muñecos, cada uno encuentra que sobran 3 centímetros ¿Cuánto mide el comedor de largo?

3.6.3. Sistemas con varias variables e igual módulo

Los sistemas de congruencias lineales con varias variables e igual módulo resultan más sencillos de resolver por su parecido a los sistemas de ecuaciones lineales.

EJEMPLO: Resolver el siguiente sistema.

$$\begin{cases} 3x + 4y \equiv 5(mod\ 13) \\ 2x + 5y \equiv 7(mod\ 13). \end{cases}$$

Dado que las congruencias lineales pueden ser combinadas linealmente sin afectación, este tipo de sistema puede ser resuelto de manera similar a los sistemas de ecuaciones lineales en variables reales. Para resolver este sistema y con el fin de eliminar la variable y, se multiplica la primera ecuación por 5 y la segunda por -4, obteniendo así el sistema

$$\begin{cases} 15x + 20y \equiv 25(mod\ 13) \\ -8x - 20y \equiv -28(mod\ 13) \end{cases}.$$

Al sumar ambas congruencias se tiene

$$7x \equiv -3 \equiv 10(mod\ 13),$$

cuya solución es

$$x \equiv 7(mod\ 13).$$

Se sustituye ahora este resultado en la primera ecuación

$$\begin{array}{r} 21x + 4y \equiv 5(mod\ 13) \\ 4y \equiv -16 \ \equiv \ -3 \equiv 10(mod\ 13) \end{array}'$$

cuya solución es

$$y \equiv 9(mod\ 13).$$

Así finalmente se obtiene la solución del sistema

$$S = \begin{cases} x \equiv 7(mod\ 13) \\ y \equiv 9(mod\ 13) \end{cases}.$$

El siguiente teorema plantea un análogo a la conocida Regla de Cramer[3].

TEOREMA 3.6.2

Sean a, b, c, d, e, f, m números enteros tales que $m > 0$ y sea

$$\Delta = ad - bc = \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

Sea además $(\Delta, m) = 1$ y $\bar{\Delta}$ el inverso módulo m de Δ. Entonces el sistema

$$\begin{cases} ax + by \equiv e(mod\ m) \\ cx - dy \equiv f(mod\ m) \end{cases}$$

tiene solución única módulo m dada por

$$\begin{cases} x \equiv \bar{\Delta}(de - bf) = \bar{\Delta} \begin{vmatrix} e & b \\ f & d \end{vmatrix} (mod\ m) \\ \\ y \equiv \bar{\Delta}(af - ce) = \bar{\Delta} \begin{vmatrix} a & e \\ c & f \end{vmatrix} (mod\ m). \end{cases}$$

Demostración: Se utiliza el método aplicado en el ejemplo. Multiplicando la primera ecuación por d y la segunda por b es

$$\begin{cases} adx + bdy & \equiv & de(mod\ m) \\ bcx - bdy & \equiv & bf(mod\ m) \end{cases}.$$

[3]Gabriel Cramer (1704-1752)

Restando se tiene

$$(ad-cb)x = \Delta x \equiv de - bf = \begin{vmatrix} e & b \\ f & d \end{vmatrix} (mod\ m),$$

de donde se obtiene la solución única módulo m (pues $(\Delta, m) = 1$)

$$x \equiv \bar{\Delta} \begin{vmatrix} e & b \\ f & d \end{vmatrix} (mod\ m).$$

Al realizar ahora el proceso análogo en el sistema original para eliminar la variable x se obtiene

$$y \equiv \bar{\Delta} \begin{vmatrix} a & e \\ b & f \end{vmatrix} (mod\ m),$$

quedando así demostrado el teorema. **Q.e.d.**

Veamos el mismo ejemplo anterior a la luz de este método:

EJEMPLO:

$$\begin{cases} 3x + 4y \equiv 5 (mod\ 13) \\ 2x + 5y \equiv 7 (mod\ 13) \end{cases}$$

Aquí es

$$\Delta = \begin{vmatrix} 3 & 4 \\ 2 & 5 \end{vmatrix} = 15 - 8 = 7 \quad \text{y} \quad (\Delta, m) = (7, 13) = 1.$$

Para hallar $\bar{\Delta}$ se soluciona la ecuación $7x \equiv 1 (mod\ 13)$, obteniendo $\bar{\Delta} = 2$. Entonces es

$$x \equiv \bar{\Delta} \begin{vmatrix} 5 & 4 \\ 7 & 5 \end{vmatrix} = 2(25 - 28) = 2(-3) = -6 \equiv 7 (mod\ 13)$$

$$y \equiv \bar{\Delta} \begin{vmatrix} 2 & 5 \\ 3 & 7 \end{vmatrix} = 2(21 - 10) = 2(11) = 22 \equiv 9 (mod\ 13)$$

.

Este método se puede generalizar a sistemas de n ecuaciones con n incógnitas. Para ello resulta necesario introducir el lenguaje de matrices. Veamos el ejemplo anterior utilizando dicho lenguaje.

$$\begin{cases} 3x + 4y \equiv 5 (mod\ 13) \\ 2x + 5y \equiv 7 (mod\ 13) \end{cases}$$

Haciendo

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix}, \quad X = \begin{pmatrix} x \\ y \end{pmatrix}, \quad B = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$$

se tiene el sistema en forma matricial $AX \equiv B(mod\ 13)$, del cual ya se conoce que

$$\Delta = \det A = 7, \quad (\Delta, m) = (7, 13) = 1 \quad \text{y} \quad \bar{\Delta} = 2.$$

Se soluciona ahora la congruencia $AX \equiv B(mod\ 13)$

$$X \equiv \bar{A}B(mod\ 13).$$

siendo $\bar{A}$ la matriz cuyos elementos son los inversos módulo 13 de los elementos correspondientes de la matriz A, es decir

$$\bar{A}B = \begin{pmatrix} 10 & -8 \\ -4 & 6 \end{pmatrix} \begin{pmatrix} 5 \\ 7 \end{pmatrix} = \begin{pmatrix} -6 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 9 \end{pmatrix} (mod\ 13),$$

de donde se obtiene la solución en forma matricial

$$X \equiv \begin{pmatrix} 7 \\ 9 \end{pmatrix} (mod\ 13).$$

DEFINICIÓN 3.6.1

*Sea A la matriz $A = (a_{ij})_{n\times n}$. Entonces la matriz $\text{adj}(A) = ((-1)^{i+j}c_{ij})_{n\times n}$ se llama **adjunta de** A, siendo c_{ij} el determinante de la matriz obtenida al tachar en A la fila i y la columna j.*

EJEMPLO:

$$A = \begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix} \quad \Longrightarrow \quad \text{adj}(A) = \begin{pmatrix} -2 & -3 & 5 \\ -5 & 0 & 10 \\ 4 & 1 & -10 \end{pmatrix}$$

El siguiente teorema resulta de gran utilidad en la resolución de sistemas de congruencias de este tipo.

TEOREMA 3.6.3

Si $A = (a_{ij})_{n\times n}$, $\Delta = \det A$ y $(\Delta, m) = 1$, entonces $\bar{A} = \bar{\Delta}(\text{adj}(A))$ es inversa de A módulo m, siendo $\bar{\Delta}$ inverso de Δ módulo m.

La demostración se realiza de modo similar al caso real y queda como ejercicio para los interesados.

DEFINICIÓN 3.6.2

*Sean $A = (a_{ij})_{n\times k}$ y $B = (b_{ij})_{n\times k}$ matrices de orden $n \times k$. Se dice que ambas **matrices** son **congruentes módulo** m (notación: $A \equiv B(mod\ m)$) si $a_{ij} \equiv b_{ij}$ para todos los valores de $i = 1, \ldots, n$ y $j = 1, \ldots, k$.*

Así se cumple (demostración como ejercicio):

TEOREMA 3.6.4

Si $A = (a_{ij})_{n\times k}$ y $B = (b_{ij})_{n\times k}$ son matrices tales que $A \equiv B(mod\ m)$, y C y D son matrices de orden $k \times p$ y $p \times n$ respectivamente, entonces es

$$AC \equiv BC(mod\ m) \quad y \quad DA \equiv DB(mod\ m).$$

Ahora el sistema de congruencias

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n & \equiv & b_1(mod\ m) \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n & \equiv & b_2(mod\ m) \\ \ldots & & \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n & \equiv & b_n(mod\ m) \end{array}$$

se transforma con la notación matricial en

$$AX \equiv B(mod\ m) \text{ siendo } A = (a_{ij})_{n\times n},\ X = (x_i)_n,\ B = (b_j)_n.$$

Entonces la técnica consiste en hallar $\bar{A}$ (inversa de A módulo m), de modo que se cumpla $\bar{A}A \equiv I(mod\ m)$, siendo I la matriz identidad de orden n.

EJEMPLO:

$$\begin{array}{rcl} 2x + 5y + 6z & \equiv & 3(mod\ 7) \\ 2x \qquad + z & \equiv & 4(mod\ 7) \\ x + 2y + 3z & \equiv & 1(mod\ 7) \end{array}$$

Aquí se tiene (ver ejemplo anterior)

$$A = \begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}, \quad \text{adj}(A) = \begin{pmatrix} -2 & -3 & 5 \\ -5 & 0 & 10 \\ 4 & 1 & -10 \end{pmatrix}, \quad \Delta = -5.$$

Como $(\Delta, 7) = (-5, 7) = 1$, se puede encontrar el inverso de Δ, siendo éste $\bar{\Delta} = 4$. Entonces es

$$\bar{A} = 4 \cdot \text{adj}(A) = \begin{pmatrix} -8 & -12 & 20 \\ -20 & 0 & 40 \\ 16 & 4 & -40 \end{pmatrix} \equiv \begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix} (mod\ 7),$$

siendo así

$$X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \equiv \begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 32 \\ 8 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} (mod\ 7).$$

En el caso de los sistemas de dos ecuaciones con dos incógnitas se puede expresar el teorema de modo más sencillo.

TEOREMA 3.6.5

Sean

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \textit{tal que} \qquad \Delta = \det A \quad y \quad (\Delta, m) = 1.$$

Entonces

$$\bar{A} = \bar{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

siendo $\bar{\Delta}$ *el inverso módulo* m *de* Δ.

Demostración:

$$\begin{aligned} A\bar{A} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bar{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \bar{\Delta} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ &= \bar{\Delta} \begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

De manera análoga se demuestra que

$$\bar{A}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Q.e.d.

3.6.4. Ejercicios

1. Solucione los sistemas de congruencias lineales siguientes:

a) $\begin{cases} x + 2y = 1 (mod\ 5) \\ 2x + y = 1 (mod\ 5) \end{cases}$ b) $\begin{cases} x + y \equiv 1 (mod\ 7) \\ x + z \equiv 2 (mod\ 7) \\ x \equiv 0 (mod\ 3) \\ y + z \equiv 3 (mod\ 7) \\ x \equiv 0 (mod\ 3) \end{cases}$

c) $\begin{cases} 2x + 2y \equiv 5 (mod\ 7) \\ x + 5y \equiv 6 (mod\ 7) \\ x \equiv 0 (mod\ 4) \end{cases}$ d) $\begin{cases} x + y + z \equiv 1 (mod\ 7) \\ x + y + w \equiv 1 (mod\ 7) \\ x + z + w \equiv 1 (mod\ 7) \\ y + z + w \equiv 1 (mod\ 7) \end{cases}$

2. Una matriz A (diferente de la identidad I) se dice **involutoria módulo** m si $A^2 \equiv I (mod\ m)$

a) Demuestre que la matriz

$$\begin{pmatrix} 4 & 11 \\ 2 & 2 \end{pmatrix}$$

es involutoria módulo 26.

b) ¿Será cierto que si una matriz cuadrada A de orden 2 es involutoria módulo m, entonces es $\det A \equiv \pm 1 (mod\ m)$?

3.7. La estructura de la clase prima de restos

Sea G_m el grupo de las clases primas de restos módulo m y sea $m = m_1 m_2 \cdots m_r$ con $m_1, m_2, \ldots, m_r$ primos relativos. Por el teorema 3.6.1 el sistema

$$x \equiv a_i (mod\ m_i) \quad (i = 1, \ldots, r)$$

tiene exactamente una solución

$$x \equiv a (mod\ m),$$

y se cumple

$$(a, m_i) = (a_i, m_i) \quad (i = 1, \ldots, r).$$

De aquí que $\overline{a}$ es una clase prima de restos módulo m si y sólo si las $\overline{a_i}$ son clases primas de restos módulo m_i.

Por el teorema 3.6.1 se tiene la representación

$$\overline{a} = \overline{a_1 e_1} + \overline{a_2 e_2} + \ldots + \overline{a_r e_r},$$

donde

$$e_k = \frac{M}{m_k} y_k, \quad M = m_1 m_2 \cdots m_n, y_k M_k \equiv 1 (mod\ m_k).$$

Sea $\overline{a_i}^*$ la clase prima de restos

$$\overline{a_i}^* = \overline{e_1 + \ldots + e_{i-1} + a_i e_i + e_{i+1} + \ldots + e_r}.$$

Entonces para cada i fijo el conjunto $G^*_{m_i}$ de las clases de restos $\overline{a_i}^*$ es un subgrupo de G_m y se cumple

$$\overline{a} = \overline{a_1}^* \cdot \overline{a_2}^* \cdots \overline{a_r}^*.$$

Desarrollando ahora este proceso para toda $\overline{a} \in G_m$ se obtiene que:

El grupo de clases primas de restos G_m es el producto directo de los subgrupos $G^*_{m_1}$, $G^*_{m_2}$, ..., $G^*_{m_r}$. Además $G^*_{m_i}$ es isomorfo a G_{m_i} a través de la relación $\overline{a_i}^* \mapsto \overline{a_i}$.

Teorema 3.7.1

Si $m = m_1 m_2 \cdots m_r$ con $m_1, m_2, \ldots, m_r$ primos relativos, entonces el grupo de las clases primas de restos módulo m es isomorfo al producto directo de los grupos de las clases primas de restos módulo m_i.

Es decir, si se considera la representación canónica de m como producto de factores primos, entonces al tener información sobre los grupos de las clases primas de restos módulo cada potencia de los factores primos, se domina toda la información sobre el grupo de las clases primas de restos módulo m.

3.8. Una aplicación de las congruencias. El calendario perpetuo

En esta sección se propone una fórmula para determinar el día de la semana de cualquier día del año. Como los días de la semana de la semana forman un ciclo de longitud 7 utilizaremos la congruencia módulo 7. Denotaremos cada día por un número entre 0 y 6 de la siguiente manera:

Domingo = 0	Lunes = 1	Martes = 2	
Miércoles = 3	Jueves = 4	Viernes = 5	Sábado = 6

Julio César sustituyó el calendario egipcio, que se basaba en exactamente 365 días, por un nuevo calendario, llamado *calendario juliano*, con un año promedio de 365.25 días, el cual contenía un año bisiesto de 366 días cada cuatro años para ajustar de ese modo el largo de los años. Sin embargo, cálculos posteriores reflejaron que el verdadero largo de los años es de 365,2422 días aproximadamente. Al pasar los siglos se fue agregando la diferencia de 0.0078 días anuales, de modo que en el año 1582 se habían agregado innecesariamente 10 días en años bisiestos. Para solucionar este problema, en 1582 el papa Gregorio creó un nuevo calendario. Primeramente se agregaron 10 días a la fecha de modo que el 5 de octubre de 1582 se convirtió en el 15 de octubre de 1582 (y se saltaron los días del 6 al 14 de octubre). Se decidió además que los años bisiestos serían exactamente los múltiplos de 4, exceptuando aquellos que son divisibles por 100 (es decir los años que marcan el cambio de siglo) de los cuales sólo serían bisiestos los divisibles por 400. Así, por ejemplo, los años 1700, 1800, 1900 y 2100 no son bisiestos mientras que 1600 y 2000 sí lo son. Con este arreglo se logra un promedio anual de 365.2425 días, el cual es más cercano al real. Se mantiene aún un error de 0.0003 días anuales, que significan 3 días en 10000 años. En el futuro se deberá tener en cuenta esta diferencia y ya existen varias proposiciones de solución.

Se debe tomar en cuenta además que el calendario gregoriano no fue adoptado en todas partes del mundo al mismo tiempo. En los Estados Unidos se adoptó el calendario gregoriano en 1752, donde se hizo necesario adicionar 11 días. Allí el

3 de septiembre de 1752 del calendario juliano se convirtió en el en el 14 de septiembre del mismo año en el calendario gregoriano. Japón cambió en 1873, Rusia y los países cercanos cambiaron en al 1917, mientras que Grecia no lo hizo hasta 1923.

Desarrollemos ahora nuestro algoritmo para encontrar el día de la semana de una fecha dada en el calendario gregoriano.

Primeramente realizaremos algunos ajustes, dado que el día adicional de los años bisiestos ocurre al final de febrero. Tomaremos este en cuenta numerando los meses, iniciando cada año en marzo y considerando los meses de enero y febrero como parte del año anterior. Así febrero de 1984 se considera el mes 12 de 1983 y mayo de 1984 es el tercer mes de 1984. Con esta convención sea

- $k =$ día del mes
- $m =$ mes , siendo

Enero $= 11$	Febrero $= 12$	Marzo $= 1$
Abril $= 2$	Mayo $= 3$	Junio $= 4$
Julio $= 5$	Agosto $= 6$	Septiembre $= 7$
Octubre $= 8$	Noviembre $= 9$	Diciembre $= 10$

- $N =$ año (aquí N es el año actual excepto en el caso en que se trate de los meses de enero o febrero, en cuyo caso N es el año anterior). Nótese además que $N = 100C + Y$.
- $C =$ indicador del siglo
- $Y =$ año particular del siglo.

EJEMPLO: Para el 3/4/1951 se tiene $k = 3, m = 2, N = 1951, C = 19, Y = 51$. Sin embargo para el 28/2/1951 se tiene $k = 28, m = 12, N = 1950$, $C = 19, Y = 50$, pues de acuerdo a nuestros cálculos febrero es considerado el mes 12 del año anterior.

Comenzaremos entonces por el primero de marzo de cada año. Sea d_N el día de la semana del 1 de marzo del año N. Comenzando por el año 1600 calcularemos el día de la semana del 1 de marzo de cualquier año dado. Nótese que entre el 1 de marzo del año $N - 1$ y el primero de marzo del año N existen 365 días, si el año no es bisiesto, y como $365 \equiv 1(\mod 7)$ se tiene que

$$d_N \equiv d_{N-1} + 1(mod\ 7),$$

Mientras que, si el el año $N - 1$ es bisiesto, entonces la diferencia es de 366 días y como $366 \equiv 2(\mod 7)$, entonces es

$$d_N \equiv d_{N-1} + 2(mod\ 7).$$

De aquí que para encontrar d_N a partir de d_{1600} debemos determinar primero cuántos años bisiestos han ocurrido entre el año 1600 y el año N (sin incluir el 1600, pero incluyendo N). Denotemos éste número por x y notemos que aplicando el algoritmo de la división se obtiene que entre 1600 y N existen

$$\begin{aligned}
&\left[\frac{N-1600}{4}\right] && \text{años que son divisibles por 4,}\\
&\left[\frac{N-1600}{100}\right] && \text{años que son divisibles por 100,}\\
&\left[\frac{N-1600}{400}\right] && \text{años que son divisibles por 400,}
\end{aligned}$$

de donde se obtiene

$$\begin{aligned}
x &= \left[\frac{N-1600}{4}\right] - \left[\frac{N-1600}{100}\right] + \left[\frac{N-1600}{400}\right]\\
&= \left[\frac{N}{4}\right] - 400 - \left[\frac{N}{100}\right] + 16 + \left[\frac{N}{400}\right] - 4\\
&= \left[\frac{N}{4}\right] - \left[\frac{N}{100}\right] + \left[\frac{N}{400}\right] - 388.
\end{aligned}$$

A escribir esta fórmula en términos de C y Y se obtiene

$$\begin{aligned}
x &= \left[25C + \frac{Y}{4}\right] - \left[C + \frac{Y}{100}\right] + \left[\frac{C}{4} + \frac{Y}{400}\right] - 388\\
&= 25C + \left[\frac{Y}{4}\right] - C + \left[\frac{C}{4}\right] - 388,
\end{aligned}$$

siendo entonces

$$x \equiv 3C + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] - 3(\quad \text{mód } 7).$$

Con esto ya se puede hallar d_N sumando un día por cada año transcurrido desde el 1600 más un día por cada año bisiesto transcurrido en esa etapa. Así es

$$\begin{aligned}
d_N &\equiv d_{1600} + N - 1600 + x (mod\ 7)\\
&\equiv d_{1600} + 100C + Y - 1600 + 3C + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] - 3 (mod\ 7).
\end{aligned}$$

Simplificando obtenemos

$$d_N \equiv d_{1600} - 2C + Y + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] (mod\ 7).$$

Hemos obtenido así una fórmula para determinar el día de la semana del primero de marzo de una año cualquiera.

Necesitaríamos saber ahora en qué día cayó el primero de marzo de 1600. Para ello utilicemos el hecho de que el primero de marzo del año 2001 es jueves (es decir $d_{2001} = 4$) para hallar d_{1600} y simplificar así la fórmula obtenida. Conociendo que para el año 2001 es $C = 20$ y $Y = 1$, según la fórmula anterior se tiene

$$\begin{aligned} 4 &\equiv d_{1600} - 2(20) + 1 + [\frac{20}{4}] + [\frac{1}{4}](mod\ 7) \\ &\equiv d_{1600} - 40 + 1 + 5 + 0(mod\ 7). \\ &\equiv d_{1600} - 34(mod\ 7), \end{aligned}$$

de donde

$$d_{1600} \equiv 38 \equiv 3(mod\ 7),$$

y así sabemos que el primero de marzo del año 1600 fue miércoles ($d = 3$).

Sustituyendo entonces en la fórmula ya conocida se obtiene la siguiente relación para determinar el día de la semana del primero de marzo del año N

$$d_N \equiv 3 - 2C + Y + \left[\frac{C}{4}\right] + \left[\frac{Y}{4}\right] (mod\ 7).$$

Usaremos ahora esta fórmula para determinar el día de la semana del primer día de cada mes del año N. Para ello debemos conocer el número de días de la semana que se corre el primero de un mes respecto al día primero del mes anterior. Los meses de 30 días trasladan en dos días al día primero del mes anterior (pues $30 \equiv 2($ mód $7)$), mientras que los de 31 días lo hacen en 3 días (pues $31 \equiv 3($ mód $7)$). Debemos entonces adicionar las siguientes cantidades:

del 1 de marzo al 1 de abril:	3 días
del 1 de abril al 1 de mayo:	2 días
del 1 de mayo al 1 de junio:	3 días
del 1 de junio al 1 de julio:	2 días
del 1 de julio al 1 de agosto:	3 días
del 1 de agosto al 1 de septiembre:	3 días
del 1 de septiembre al 1 de octubre:	2 días
del 1 de octubre al 1 de noviembre:	3 días
del 1 de noviembre al 1 de diciembre:	2 días
del 1 de diciembre al 1 de enero:	3 días
del 1 de enero al 1 de febrero:	3 días.

Necesitamos una fórmula que nos produzca esos incrementos. Nótese que tenemos 11 incrementos con un total de 29 días, de modo que cada incremento promedia 2,6 días. Se puede comprobar que la función $[2{,}6m - 0{,}2] - 2$ tiene exactamente los mismos incrementos al recorrer m los números del 2 al 12 y vale 0 cuando $m = 1$. (Esta fórmula fue descubierta originalmente por el reverendo Séller, el cual aparentemente

la encontró por ensayo y error). Entonces el día de la semana del primer día del mes m del año N está dado por el menor resto no negativo de $d_N + [2{,}6m - 0{,}2] - 2$ módulo 7.

Ahora, para encontrar W (día de la semana del día k del mes m del año N) solamente debemos adicionar $k-1$ a la fórmula obtenida para el día de la semana del primer día del mes m. Así se obtiene la fórmula:

$$W \equiv k + [2.6m - 0.2] - 2C + Y + \left[\frac{Y}{4}\right] + \left[\frac{C}{4}\right] (mod\ 7).$$

La fórmula así obtenida nos servirá como calendario perpetuo para determinar el día de la semana de cualquier fecha.

EJEMPLO: Determine el día de la semana del 1/1/1900.

Aquí es $k = 1, m = 11, N = 1899, C = 18, Y = 99$. Aplicando la fórmula se obtiene

$$\begin{aligned} W &\equiv 1 + [(2{,}6)11 - 0{,}2] - 2(18) + 99 + [\frac{99}{4}] + \left[\frac{18}{4}\right] (mod\ 7) \\ &\equiv 1 + [28{,}4] - 36 + 99 + [24{,}75] + [4{,}5](mod\ 7) \\ &\equiv 1 + 28 - 36 + 99 + 24 + 4(mod\ 7) \\ &\equiv 120(mod\ 7) \\ &\equiv 1(mod\ 7). \end{aligned}$$

Es decir, el día 1/1/1900 fue lunes.

3.8.1. Ejercicios

1. Determine el día de la semana de su cumpleaños en el año actual.
2. Determine el año más próximo en que su cumpleaños será un sábado.
3. Determine cuántos martes 13 habrá en este año.

3.9. Ejercicios del capítulo

1. Demuestre que un número natural es divisible por 13, 17 y 19 si y sólo si al formar la suma de 4 veces, -5 veces y el doble de la última con el número restante del desarrollo decimal del número dado, la suma es divisible por 13, 17 y 19.
2. Encuentre todas las soluciones de las ecuaciones diofánticas
   a) $255x + 83y = 202$

b) $137952x + 1743y = 415612$

c) $10x + 18y + 15z = 404$

3. Determine el conjunto de los divisores primos de 9, 99, 999, ...

4. Considere la sucesión $\{n^n\}_{n\geq 1}$ módulo p primo. Demuestre que la sucesión de clases de restos es periódica y halle la longitud del período.

5. Halle todos los n tales que $\phi(n) = 1, 2, 3, 4, 5, 6, 14$.

6. Sea p_n el n-ésimo nímero primo. Demuestre que:

   a) Se cumple que
   $$\frac{\phi(p_n!)}{p_n!} \cdots \frac{p_{n-1}!}{\phi(n-1!)} = 1 - \frac{1}{p_n}.$$

   b) Si $k = \prod_{i=1}^{n} p_i^{\nu_i}$ con $\nu_i \geq 1$ para $i = 1, 2, \ldots, n$, entonces
   $$\frac{\phi(k)}{k} = \frac{\phi(p_n!)}{p_n!}.$$

7. Demuestre que $\phi(n) \geq \frac{1}{2}\sqrt{n}$ para todo natural n.

8. Demuestre que $\phi(n) \neq n - \sqrt{n}$ para todo natural n.

9. Demuestre que existen infinitos números primos con $\phi(n) > \phi(n+1)$.

10. Demuestre la identidad
    $$\phi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right].$$

11. Demuestre las siguientes proposiciones

    a) Si $a \equiv b(mod\ n)$ y $m|n$, entonces $a \equiv b(mod\ m)$.

    b) Si $a \equiv b(mod\ n)$ y $c > 0$, entonces $ca \equiv cb(mod\ cn)$.

    c) Si $a \equiv b(mod\ n)$ y los enteros a, b, n son todos divisibles por $d > 0$, entonces $\frac{a}{d} \equiv \frac{b}{d}\left(mod\ \frac{n}{d}\right)$.

12. Muestre con un ejemplo que $a^2 \equiv b^2(mod\ n)$ no implica necesariamente que $a \equiv b(mod\ n)$.

13. Si $a \equiv b(mod\ n)$, demuestre que $(a, n) = (b, n)$.

14. *a*) Determine los restos al dividir 2^{50} y 41^{65} por 7.

b) ¿Cuál es el resto cuando la suma

$$1^5 + 2^5 + \ldots + 100^5$$

se divide por 4?

15. Si $\{a_1, a_2, \ldots, a_n\}$ es un sistema completo de restos módulo n y $(a, n) = 1$, demuestre que $\{aa_1, aa_2, \ldots, aa_n\}$ es un sistema completo de restos módulo n. (Sugerencia: basta demostrar que esos números son incongruentes módulo n).

16. Compruebe que $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ forman un sistema completo de restos módulo 11, pero $0, 1^2, 2^2, 3^2, \ldots, 10^2$ no.

17. Demuestre las siguientes proposiciones

a) Si $(a, n) = 1$, entonces los enteros

$$c,\ c + a,\ c + 2a,\ c + 3a, \ldots, c + (n-1)a$$

forman un sistema completo de restos módulo n para todo c.

b) Si $a \equiv b(mod\ n)$ y $c > 0$, entonces $ca \equiv cb(mod\ cn)$.

c) Cualesquiera n enteros consecutivos forman un sistema completo de restos módulo n (Sugerencia: use el inciso anterior).

d) El producto de cualquier conjunto de n enteros consecutivos es divisible por n.

18. Demuestre que $a \equiv b(mod\ n_1)$ y $a \equiv b(mod\ n_2)$ implica $a \equiv b(mod\ n)$, donde $n = [n_1, n_2]$. Luego, si n_1 y n_2 son primos relativos, entonces $a \equiv b(mod\ n_1 n_2)$.

19. Muestre con un ejemplo que $a^k \equiv b^k(mod\ n)$ y $k \equiv j(mod\ n)$ no implica necesariamente que $a^j \equiv b^j(mod\ n)$.

20. Demuestre las siguientes proposiciones

a) Si a es un entero impar, entonces $a^2 \equiv 1(mod\ 8)$.

b) Para todo entero a es $a^3 \equiv 0, 1$ o $8(mod\ 9)$.

c) Para todo entero a es $a^3 \equiv a(mod\ 6)$.

d) Si un entero a no es divisible por 2 o 3, entonces $a^2 \equiv 1(mod\ 24)$.

e) Si un entero a es a la vez cuadrado y cubo, entonces $a \equiv 0, 1, 9$ ó $28(mod\ 36)$.

21. Demuestre que si a es un entero impar, entonces

$$a^{2^n} \equiv 1(mod\ 2^{n+2})$$

para todo $n \geq 1$ (Sugerencia: proceda por inducción en n).

22. Mediante la teoría de congruencias compruebe que $89|2^{44}-1$ y $97|2^{48}-1$.

23. Demuestre que si $ab \equiv cd(mod\ n)$ y $b \equiv d(mod\ n)$ con $(b,n)=1$, entonces $a \equiv c(mod\ n)$.

24. Si $a \equiv b(mod\ n_1)$ y $a \equiv c(mod\ n_2)$, demuestre que $b \equiv c(mod\ n)$, donde $n=(n_1,n_2)$.

25. Demuestre las proposiciones siguientes:

    a) Para todo entero a, el dígito de las unidades de a^2 es $0,1,4,5,6$ ó 9.

    b) Cualquiera de los enteros $0,1,2,3,4,5,6,7,8,9$ puede ser el dígito de las unidades de a^3.

    c) Para todo entero a, el dígito de las unidades de a^4 es $0,1,5,6$ ó 6.

    d) El dígito de las unidades de un número triangular es $0,1,3,5,6$ ó 8.

26. Halle los dos últimos dígitos de 9^{9^9}. (Sugerencia: $9^9 \equiv 9(mod\ 10)$, por lo que $9^{9^9} \equiv 9^{9+10k}(mod\ 10)$, use ahora el hecho de que $9^{10} \equiv 1(mod\ 100)$).

27. Sin desarrollar las divisiones, determine si los enteros 176 521 221 y 149 235 678 son divisibles por 9 y 11.

28. *a*) Obtenga la siguiente generalización del teorema referido a las congruencias de polinomios: Si el entero N es representado en la base b

$$N = a_m b^m + \ldots + a_2 b^2 + a_1 b + a_0, \qquad 0 \leq a_k \leq b-1,$$

    entonces $b-1|N$ si y sólo si $b-1|(a_0+a_1+a_2+\ldots+a_m)$.

    b) Encuentre criterios de divisibilidad de N por 3 y por 8 que dependan de la representación de N en base 9.

    c) Analice si el entero 447836 es divisible por 3 y por 8.

29. Usando el test de visibilidad por 9 y por 11 encuentre los dígitos "x" faltantes:

    a) $52817 \cdot 3212146 = 169655x15282$

    b) $2x99561 = [3(523+x)]^2$

30. Establezca los siguientes criterios de divisibilidad:

    a) Un entero es divisible por 2 si y sólo si el dígito de las unidades es $0,2,4,6$ ó 8.

    b) Un entero es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

c) Un entero es divisible por 4 si y sólo si el número formado por los dígitos de las decenas y unidades es divisible por 4 (Sugerencia: $10^k \equiv 0(mod\ 4)$ para $k \geq 2$).

d) Un entero es divisible por 5 si y sólo si el dígito de las unidades es 0 ó 5.

31. Demuestre que 2^n divide a un entero N si y sólo si 2^n divide al número formado con los últimos n dígitos de N (Sugerencia: $10^k = 2^k 5^k \equiv 0(mod\ 2^n)$ para $k \geq n$).

32. Sea $N = a_m 10^m + \ldots + a_2 10^2 + a_1 10 + a_0$ con $0 \leq a_k \leq 9$ la expansión decimal de un entero positivo N. Demuestre que 7, 11 y 13 dividen simultáneamente a N si y sólo si 7, 11 y 13 dividen simultáneamente al entero

$$M = (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \ldots$$

(Sugerencia: Si n es par, entonces $10^{3n} \equiv 1(mod\ 1001)$, $10^{3n+1} \equiv 10(mod\ 1001)$, $10^{3n+2} \equiv 100(mod\ 1001)$; si n es impar, entonces $10^{3n} \equiv -1(mod\ 1001)$, $10^{3n+1} \equiv -10(mod\ 1001)$, $10^{3n+2} \equiv -100(mod\ 1001)$).

33. Sin realizar la división, determine si el entero 1 010 908 899 es divisible por 7, 11 y 13.

34. *a*) Dado un entero N, sea M el entero formado a invertir el orden de los dígitos de N (por ejemplo, si $N = 6923$, entonces $M = 3296$). Demuestre que $N - M$ es divisible por 9.

b) Un *palíndromo* o *capicúa* es un número que se lee igual de izquierda a derecha que de derecha a izquierda (por ejemplo, 373 y 521125 son palíndromos). Demuestre que todo palíndromo con un número par de dígitos es divisible por 11.

c) Demuestre que todos los enteros

$$1111, \quad 111111, \quad \ldots, 11\ldots11,$$

con un número par de dígitos son compuestos

35. Explique por qué se cumplen los siguientes cálculos curiosos

$$\begin{aligned}
1 \cdot 9 + 2 &= 11 \\
12 \cdot 9 + 3 &= 111 \\
123 \cdot 9 + 4 &= 1\ 111 \\
1234 \cdot 9 + 5 &= 11\ 111 \\
12345 \cdot 9 + 6 &= 111\ 111 \\
123456 \cdot 9 + 7 &= 1\ 111\ 111 \\
1234567 \cdot 9 + 8 &= 11\ 111\ 111 \\
12345678 \cdot 9 + 9 &= 111\ 111\ 111 \\
123456789 \cdot 9 + 10 &= 1\ 111\ 111\ 111.
\end{aligned}$$

(Sugerencia: Compruebe que

$$(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \ldots + n)(10 - 1) + (n - 1) = \frac{10^{n+1} - 1}{9}\Big).$$

36. Una factura vieja y algo ilegible dice que se compraron 72 jamones en conserva por \$ $x67,9$. Halle el dígito "x" faltante.

37. Resuelva las siguientes congruencias lineales:

    a) $25x \equiv 15(mod\ 29)$

    b) $5x \equiv 2(mod\ 26)$

    c) $6x \equiv 15(mod\ 21)$

    d) $36x \equiv 8(mod\ 102)$

    e) $34x \equiv 60(mod\ 98)$

    f) $140x \equiv 133(mod\ 301)$ (Sugerencia: $(140, 301) = 7$).

38. Usando congruencias, solucione las siguientes ecuaciones diofánticas:

    a) $4x + 51y = 9$ (Sugerencia: $4x \equiv 9(mod\ 51)$ implica $x = 15 + 51t$, mientras $51y \equiv 9(mod\ 4)$ implica $y = 3 + 4s$, halle la relación entre s y t).

    b) $12x + 25y = 331$

    c) $5x - 53y = 17$

39. Halle todas las soluciones de la congruencia lineal $3x - 7y \equiv 11(mod\ 13)$.

40. Soluciones los siguientes sistemas de congruencias

    a) $x \equiv 1(mod\ 3), \quad x \equiv 2(mod\ 5), \quad x \equiv 3(mod\ 7)$

    b) $x \equiv 5(mod\ ll), \quad x \equiv 14(mod\ 29), \quad x \equiv 15(mod\ 31)$

    c) $x \equiv 5(mod\ 6), \quad x \equiv 4(mod\ ll), \quad x \equiv 3(mod\ 17)$

    d) $2x \equiv 1(mod\ 5), \quad 3x \equiv 9(mod\ 6), \quad 4x \equiv 1(mod\ 7), \quad 5x \equiv 9(mod\ 11)$

41. Solucione la congruencia lineal $17x \equiv 3(mod\ 2 \cdot 3 \cdot 5 \cdot 7)$, solucionando el sistema

$$\begin{array}{l} 17x \equiv 3(mod\ 2) \\ 17x \equiv 3(mod\ 3) \\ 17x \equiv 3(mod\ 4) \\ 17x \equiv 3(mod\ 7) \end{array}.$$

42. Halle el menor entero $a > 2$ tal que

$$2|a, \quad 3|a + 1, \quad 4|a + 2, \quad 5|a + 3, \quad 6|a + 4.$$

43. *a*) Obtenga tres enteros consecutivos que tengan cada uno un factor cuadrado (Sugerencia: halle un entero tal que $2^2|a$, $3^2|a+1$, $5^2|a+2$).

    b) Obtenga tres enteros consecutivos, el primero de los cuales sea divisible por un cuadrado, el segundo por un cubo y el tercero por una potencia cuarta.

44. (Brahmagupta, siglo VII A.C.) Cuando se sacan huevos de una cesta en grupos de $2, 3, 4, 5, 6$, quedan respectivamente $1, 2, 3, 4, 5$ huevos. Cuando se sacan los huevos en grupos de a 7, no queda ninguno. Halle el menor número de huevos que puede contener la cesta.

45. El problema de la cesta de huevos es variado a menudo de la siguiente manera: Siempre que los huevos son sacados de la cesta en grupos de a $2, 3, 4, 5$ o 6, queda un huevo, pero no queda ninguno si se sacan en grupos de a 7. Halle el menor número de huevos que puede contener la cesta.

46. (Antiguo problema chino). Una banda de 17 piratas robó un saco de monedas de oro. Al tratar de dividir la fortuna en porciones iguales sobraron 3 monedas. En la reyerta por obtener las monedas sobrantes un pirata fue asesinado. La riqueza se distribuyó, sobrando ahora 10 monedas tras el reparto equitativo. Otra vez la discusión provocó que un pirata fuera muerto. Pero ahora la fortuna total pudo ser distribuida equitativamente entre los sobrevivientes ?cuál es el menor número posible de monedas robadas?

47. Demuestre que las congruencias

$$x \equiv a(mod\ n) \quad \text{y} \quad x \equiv b(mod\ m)$$

    admiten una solución simultánea si y sólo si $(n, m)|(a - b)$. Si existe solución conpruebe que es única módulo $[n, m]$.

48. Use el problema anterior para comprobar que el sistema

$$\begin{aligned} x &\equiv 5(mod\ 6) \\ x &\equiv 7(mod\ 15) \end{aligned}$$

    no tiene solución.

49. Si $x \equiv a(mod\ n)$, demuestre que $x \equiv a(mod\ 2n)$ ó $x \equiv a + n(mod\ 2n)$.

50. Un cierto entero entre 1 y 1200 deja los restos $1, 2, 6$ al ser dividido por $9, 11, 13$ respectivamente. ¿cuál es el número?

51. *a*) Encuentre un entero que deje restos $1, 2, 5, 5$ al ser dividido por $2, 3, 6, 12$ respectivamente (Yih-Hing, fallecido en 717).

b) Encuentre un entero que deje restos $2, 3, 4, 5$ al ser dividido por $3, 4, 5, 6$ respectivamente (Bhaskara, nacido en 1114).

c) Encuentre un entero que deje restos $3, 11, 15$ al ser dividido por $10, 13, 17$ respectivamente (Regiomontanus, 1436-1473).

52. Compruebe que $18^6 \equiv 1(mod\ 7^k)$ para $k = 1, 2, 3$.

53. *a*) Si $(a, 35) = 1$, demuestre que $a^{12} \equiv 1(mod\ 35)$ (Sugerencia: por el Teorema de Fermat es $a^6 \equiv 1(mod\ 7)$ y $a^4 \equiv 1(mod\ 5)$).

b) Si $(a, 42) = 1$, demuestre que $168 = 3 \cdot 7 \cdot 8$ divide a $a^6 - 1$.

c) Si $(a, 133) = (b, 133) = 1$, demuestre que $133|a^{18} - b^{18}$.

54. Demuestre que existen infinitos números compuestos n tales que $a^{n-1} \equiv a(mod\ n)$ (Sugerencia: hacer $n = 2p$, donde p es primo impar).

55. Demuestre las siguientes congruencias:

a) $a^{21} \equiv a(mod\ 15)$ para todo a (Sugerencia: por el Teorema de Fermat es $a^5 \equiv a(mod\ 5)$).

b) $a^7 \equiv a(mod\ 42)$ para todo a

c) $a^{13} \equiv a(mod\ 3 \cdot 7 \cdot 13)$ para todo a

56. Para todo entero a, demuestre que a^5 y a tiene igual dígito de las unidades.

57. Halle el dígito de las unidades de 3^{100} aplicando el Teorema de Fermat (Sugerencia: $3^{100} = 3(3^9)^{11}$).

58. Demuestre las siguientes congruencias para todo entero positivo n:

a) $a^{2n} \equiv a(mod\ 3)$

b) $a^{3n} \equiv a(mod\ 7)$

c) $a^{4n} \equiv a(mod\ 17)$

59. *a*) Sea p primo y $(a, p) = 1$. Aplique el Teorema de Fermat's para comprobar que $x \equiv a^{p-2}b(mod\ p)$ es una solución de la congruencia $ax \equiv b(mod\ p)$.

b) Usando el inciso anterior, solucione las congruencias $2x \equiv 1(mod\ 31)$, $6x \equiv 5(mod\ 11)$ y $3x \equiv 17(mod\ 29)$.

60. Asumiendo que a y b son enteros no divisibles por el primo p, establezca lo siguiente:

a) Si $a^p \equiv b^p(mod\ p)$, entonces $a \equiv b(mod\ p)$.

b) Si $a^p \equiv b^p(mod\ p)$, entonces $a^p \equiv b^p(mod\ p^2)$ (Sugerencia: por a) se tiene que $a = b + pk$ para cierto k, de donde $a^p - b^p = (b + pk)^p - b^p$, compruebe que p^2 divide a la última expresión).

61. Utilice el Teorema de Fermat parademostrar que si p es primo impar, entonces

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

    b) $1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 0 (mod\ p)$ (Sugerencia: utilice la identidad conocida para la suma de los primeros $p-1$ números).

62. Demuestre que si p es primo impar y k es un entero con $1 \leq k \leq p-1$, entonces el coeficiente binomial

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

63. Asuma que p y q son primos impares diferentes tales que $(p-1)|(q-1)$. Si $(a, pq) = 1$, demuestre que $a^{q-1} \equiv 1 (mod\ pq)$.

64. Si p y q son primos diferentes, demuestre que

$$p^{q-1} + q^{p-1} \equiv 1 (mod\ pq).$$

65. Compruebe que los enteros $1729 = 7 \cdot 13 \cdot 19$ y $1905 = 3 \cdot 5 \cdot 127$ son pseudoprimos.

66. Demuestre que $561|2^{561} - 2$ y $561|3^{561} - 3$. Una pregunta aún sin respuesta es la que se refiere a la existencia de finitos o infinitos enteros n con la propiedad de que $n|2^n - 2$ y $n|3^n - 3$.

67. *a*) Halle el resto al dividir 15! por 17.

    b) Halle el resto al dividir 2(26!) por 29 (Sugerencia: por el Teorema de Wilson es $2(p-3)! \equiv -1 (mod\ p)$ para todo primo impar $p > 3$).

68. Determine si 17 es primo, comprobando si se cumple $16! \equiv -1 (mod\ 17)$.

69. Ordene los enteros $2, 3, 4, \ldots, 21$ en pares a y b con la propiedad $ab \equiv 1 (mod\ 23)$.

70. Compruebe que $18! \equiv -1 (mod\ 437)$.

71. *a*) Demuestre que un entero $n > 1$ es primo si y sólo si $(n-2)! \equiv 1 (mod\ n)$.

    b) Si n es un entero compuesto, demuestre que $(n-1)! \equiv 0 (mod\ n)$ excepto en el caso $n = 4$.

72. Dado un número primo p demuestre la congruencia

$$(p-1)! \equiv (p-1) (mod\ 1 + 2 + 3 + \ldots + (p-1)).$$

73. Si p es primo, demuestre que

$$p|a^p + (p-1)!a \qquad \text{y} \qquad p|(p-1)!a^p + a$$

para todo entero a (Sugerencia: por el Teorema de Wilson se tiene la congruencia $a^p + (p-1)!a \equiv a^p - a (mod\ p)$).

74. Halle dos primos impares $p \leq 13$ para los cuales se cumpla la congruencia $(p-1)! \equiv 1(mod\ p^2)$.

75. Usando el Teorema de Wilson, demuestre que

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p-1}{2}} (mod\ p).$$

para todo primo impar p (Sugerencia: como $k \equiv -(p-k)(mod\ p)$, se tiene que $2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{\frac{p-1}{2}} 1 \cdot 3 \cdot 5 \cdots (p-2)(mod\ p)$).

Capítulo 4

DE LAS RAÍCES PRIMITIVAS A LOS RESIDUOS CUADRÁTICOS

4.1. Raíces primitivas

Por el teorema de Fermat-Euler, para todos $a, m \in \mathbb{Z}$ con $m > 1$ y $(a, m) = 1$ existe al menos un $d \in \mathbb{N}$ con $a^d \equiv 1(mod\ m)$ y ya se ha visto que $d|\phi(m)$. Por otra parte, lo ejemplos $7^6 \equiv 1(mod\ 43)$ y $5^n \not\equiv 1(mod\ 7)$ para todo $1 \leq n < 6$ muestran que puede ser $d < \phi(m)$ o $d = \phi(m)$. A partir de ello se define

DEFINICIÓN 4.1.1

*Se dice que d es el **orden de** a **módulo** m o que a **pertenece módulo** m **al exponente** d si se cumple*

$$\begin{aligned} a^d &\equiv 1(mod\ m) \\ a^n &\not\equiv 1(mod\ m) \quad \forall\ 1 \leq n < d. \end{aligned}$$

Notación: $d = ord_m a$.

EJEMPLO:

$$\begin{aligned} 2^1 &= 2 \equiv 2(mod\ 7) \\ 2^2 &= 4 \equiv 4(mod\ 7) \\ 2^3 &= 8 \equiv 1(mod\ 7), \end{aligned}$$

de modo que $3 = ord_7 2$.

Se trata de hallar la menor solución positiva de $a^x \equiv 1(mod\ m)$ para $(a, m) = 1$.

TEOREMA 4.1.1

Sean a, m enteros positivos con $(a, m) = 1$. Entonces x es solución de la congruencia $a^x \equiv 1(mod\ m)$ si y solo si $ord_m a|x$.

Demostración: (Necesidad) Para $a^x \equiv 1(mod\ m)$, sea $x = q \cdot ord_m a + r$ con $0 \leq r < ord_m a$. Entonces es

$$a^x = a^{q \cdot ord_m a + r} = \left(a^{ord_m a}\right)^q a^r \equiv a^r (mod\ m).$$

Pero entonces $a^r \equiv 1(mod\ m)$ y como $0 \leq r < ord_m a$, tiene que ser $r = 0$. Luego $x = q \cdot ord_m a$, con lo cual $ord_m a | x$.

(Suficiencia) Si $ord_m a | x$, entonces es $x = q \cdot ord_m a$ con q entero. De ahí que sea

$$a^x = a^{q \cdot ord_m a} = \left(a^{ord_m a}\right)^q \equiv 1(mod\ m).$$

Q.e.d.

EJEMPLO: Como $2^3 \equiv 1(mod\ 7)$, entonces

- como 3 no divide a 10, se tiene que $2^{10} \not\equiv 1(mod\ 7)$;
- como 3 divide a 15, se tiene que $2^{15} \equiv 1(mod\ 7)$.

Corolario 4.1.1

Sean a, m enteros positivos con $(a, m) = 1$ y $m > 1$. Entonces $a^i \equiv a^j (mod\ m)$ si y solo si $i \equiv j (mod\ ord_m a)$. De aquí que los números

$$1, a, a^2, \ldots, a^{d-1}$$

son incongruentes módulo m, siendo $d = ord_m a$.

Demostración: (Necesidad) Sea $a^i \equiv a^j (mod\ m)$ con $i \geq j$. Como $(a, m) = 1$, se tiene que $(a^i, m) = 1$ y $a^i \equiv a^j a^{i-j} \equiv a^j (mod\ m)$, de donde $a^{i-j} \equiv 1(mod\ m)$. Entonces $ord_m a | (i - j)$, con lo cual y por ello $i \equiv j (mod\ ord_m a)$.

(Suficiencia) Sea $i \equiv j (mod\ ord_m a)$ con $0 \leq j \leq i$. Entonces $i = j + k \cdot ord_m a$ para cierto entero k, con lo cual es

$$a^i \equiv a^{j + k \cdot ord_m a} \equiv a^j (mod\ m),$$

quedando así demostrado el corolario. **Q.e.d.**

Corolario 4.1.2

Si $d = ord_m a$ y $n \in \mathbb{N}$ con $(n, d) = 1$, entonces $ord_m a^n = d$.

Demostración: Sea $ord_m a^n = t$, es decir,

$$(a^n)^t \equiv 1(mod\ m).$$

Por el teorema 4.1.1 $d|nt$. Pero $(n,d)=1$ implica que $d|t$, de donde $d \leq t$.

Por otra parte,

$$(a^n)^d = (a^d)^n \equiv 1(mod\ m),$$

de donde $d \geq t$. Con ello queda demostrado que $t = d$. **Q.e.d.**

A partir de este concepto se define la raíz primitiva de un entero positivo.

DEFINICIÓN 4.1.2

Un entero r, primo relativo con el entero $m > 1$, tal que $ord_m r = \phi(m)$ se llama ***raíz primitiva módulo*** m.

EJEMPLO: 5 es raíz primitiva módulo 7, pues $ord_7 5 = 6 = \phi(7)$. Pero 7 no es raíz primitiva módulo 43, pues $ord_{43} 7 = 6 \neq 42 = \phi(43)$.

El teorema siguiente muestra una forma práctica de obtener un sistema reducido de restos a partir de una raíz primitiva módulo m.

TEOREMA 4.1.2

Si r es una raíz primitiva módulo m. Entonces $\{r^1, r^2, \ldots, r^{\varphi(m)}\}$ es un sistema reducido de restos módulo m.

Demostración: Como $(m,r)=1$, entonces $(m,r^k)=1$ para todo entero positivo k, por lo que todos los elementos del sistema $\{r^1, r^2, \ldots, r^{\varphi(m)}\}$ son primos relativos con m.

Si fuera $r^i \equiv r^j(mod\ m)$, siendo $(m,r)=1$ y $ord_m r = \varphi(m)$, tiene que ser $i \equiv j(mod\ \varphi(m))$. Pero esto es contradictorio, pues $1 \leq i,j \leq \varphi(m)$, de modo que $r^i \not\equiv r^j(mod\ m)$. **Q.e.d.**

La propiedad siguiente del orden de un entero respecto a un módulo, será de utilidad en el trabajo con las raíces primitivas.

TEOREMA 4.1.3

Si $ord_m a = t$ y u es un entero positivo, entonces es

$$ord_m\,(a^u) = \frac{t}{(t,u)}.$$

Demostración: Sean

$$s = ord_m\,(a^u), \quad (m,r)=1, \quad v=(t,u), \quad t = t_1 v, \quad u = u_1 v.$$

Como $v=(t,u)$, se tiene que $(t_1,u_1)=1$. Entonces

$$(a^u)^{t_1} = (a^{u_1 v})^{\frac{t_1}{v}} = (a^{u_1})^t = \left(a^t\right)^{u_1} \equiv 1(mod\ m),$$

por lo que s divide a t_1.

Por otra parte
$$(a^u)^s = a^{us} \equiv 1(mod\ m),$$

y t divide a us, de modo que t_1 divide a $u_1 vs$ y por tanto a $u_1 s$ y como $(m, r^k) = 1$ para $(t_1, u_1) = 1$, entonces t_1 divide a s. De todo lo anterior se tiene

$$s = t_1 = \frac{t}{v} = \frac{t}{(t,u)}.$$

Q.e.d.

EJEMPLO:
$$ord_7 3^4 = \frac{6}{(6,4)} = \frac{6}{2} = 3.$$

Corolario 4.1.3

Si r es raíz primitiva módulo $m > 1$, entonces r^u es raíz primitiva módulo m si y solo si $(u, \varphi(m)) = 1$.

Demostración: Se cumple que

$$ord_m\left(r^u\right) = \frac{ord_m r}{(ord_m r, u)} = \frac{\varphi(m)}{(\varphi(m), u)},$$

de modo que $ord_m(r^u) = \varphi(m)$ si y solo si $(u, \varphi(m)) = 1$. **Q.e.d.**

Un tema de interés se refiere a la posible cantidad de raíces primitivas.

Teorema 4.1.4

Para todo módulo m existen $\phi(\phi(m))$ raíces primitivas incongruentes o ninguna.

Demostración: Sea r una raíz primitiva módulo m. Por el teorema 4.1.2 la familia $\{r^1, r^2, \ldots, r^{\varphi(m)}\}$ es un sistema reducido de restos módulo m. De ello se deduce que r^u es también raíz primitiva módulo m y por tanto es $(u, \phi(m)) = 1$. Pero existen $\phi(\phi(m))$ números de ese tipo con $n \leq \phi(m)$.

Por otra parte, si ν recorre los números 0 hasta $\phi(m)-1$, entonces r^ν recorre el sistema reducido de restos módulo m (teorema 4.1.2). Si ν es tal que $(\nu, \phi(m)) = t > 1$, entonces
$$(r^\nu)^{\phi(m)} \equiv 1(mod\ m),$$

por lo que r no es raíz primitiva módulo m. **Q.e.d.**

EJEMPLO: 2 es raíz primitiva módulo 11, con lo cual 11 tiene $\phi(\phi(11)) = 4$ raíces primitivas incongruentes, que son 2, 6, 7, 8.

Surge ahora de modo natural la pregunta sobre cuáles enteros tienen raíz primitiva. Veamos primeramente el caso de los números primos.

RAÍCES PRIMITIVAS DE NÚMEROS PRIMOS

DEFINICIÓN 4.1.3

Sea $f(x)$ un polinomio con coeficientes enteros. Se dice que un entero c ***es raíz de f módulo*** *m si $f(c) \equiv 0(mod\ m)$.*

Note que si c es raíz de f módulo m, entonces todo número congruente a c módulo m también lo es.

EJEMPLO: El polinomio $f(x) = x^2 + x + 1$ tiene exactamente dos raíces incongruentes módulo 7, que son $x \equiv 2(mod\ 7)$ y $x \equiv 4(mod\ 7)$. Sin embargo, $g(x) = x^2+2$ no tiene raíces módulo 5.

Por otra parte, según el pequeño teorema de Fermat $h(x) = x^{p-1}-1$ tiene exactamente $p-1$ raíces incongruentes módulo p, si p es primo. Compárese al respecto el siguente teorema de Lagrange[1] con el Teorema Fundamental del Álgebra.

TEOREMA 4.1.5 ***Lagrange***

Sea $f(x) = a_n x^n + \ldots + a_1 + a_0$ un polinomio de grado n, p un número primo, $n > 0$ y a_k entero para todo índice k tal que p no divide a a_n. Entonces f tiene a lo sumo n raíces incongruentes módulo p.

Demostración: (Por inducción sobre el grado de f)

(1) Si $n = 1$, es $f(x) = a_1x+a_0$ y p no divide a a_1. De aquí que $a_1x+a_0 \equiv 0(mod\ p)$, es decir $a_1x \equiv -a_0(mod\ p)$. Pero p no divide a a_1, por lo que $(a_1, p) = 1$ y por ello existe una única solución.

(2) Supongamos que el teorema es válido para f de grado $n-1$.

(3) Sea ahora f de grado n, tal que p no divide a a_n. Supongamos además que f tiene $n+1$ raíces incongruentes módulo p. Sean $c_0, c_1, \ldots, c_n$ dichas raíces. Entonces, como $x^k - c_0^k = (x - c_0)h(x)$ con $grh(x) = k - 1$, se tiene

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \ldots + a_1(x - c_0) \\ &= (x - c_0)g(x), \end{aligned}$$

[1] Joseph Louis Lagrange (1736-1813)

siendo $g(x)$ un polinomio de grado $n-1$, el cual según el punto (2) tiene a lo sumo $n-1$ raíces. Entonces para todo índice $1 \leq k \leq n$ es

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0(mod\ p),$$

de donde, teniendo en cuenta que c_k y c_0 son incongruentes módulo p, se deduce que

$$g(c_k) \equiv 0(mod\ p).$$

Entonces $c_0, c_1, \ldots, c_n$ son n raíces de $g(x)$, lo cual contradice el hecho de que $g(x)$ tiene a lo sumo $n-1$ raíces. **Q.e.d.**

TEOREMA 4.1.6

Sea p un número primo y d un divisor de $p-1$. Entonces x^d-1 tiene exactamente d raíces incongruentes módulo p.

Demostración: Sea $p-1 = dk$. Entonces es

$$\begin{aligned} x^{p-1} - 1 &= x^{dk} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1) \\ &= x^{d(k-1)}g(x). \end{aligned}$$

Pero según el pequeño teorema de Fermat $x^{p-1} - 1$ tiene $p-1$ raíces incongruentes modulo p, por lo que cada raíz de $x^{p-1} - 1$ lo es también de $x^d - 1$ o de $g(x)$.

Pero el teorema de Lagrange afirma que g tiene a lo sumo $d(k-1)$ raíces incongruentes módulo p. Además es $d(k-1) = p - d - 1$.

Como toda raíz de $x^{p-1} - 1$ que no lo sea de $g(x)$ tiene que serlo de $x^d - 1$, entonces x^d-1 tiene como mínimo $(p-1)-(p-d-1) = d$ raíces incongruentes módulo p.

Por otro lado, según el teorema de Lagrange $x^d - 1$ tiene a lo sumo d raíces incongruentes módulo p, quedando así demostrado el teorema. **Q.e.d.**

Con la ayuda de la función φ de Euler se determina el número de enteros de orden d módulo p primo, como muestra el teorema siguiente.

TEOREMA 4.1.7

Si p es un número primo y d es un divisor de $p-1$, entonces el número de enteros de orden d módulo p incongruentes es $\varphi(d)$.

Demostración: Sea $F(d)$ el número de enteros menores que p que son de orden d módulo p. Entonces es

$$p - 1 = \sum_{d|p-1} F(d),$$

pues el orden módulo p de un entero no divisible por p divide a $p-1$. Además se conoce que

$$p-1=\sum_{d|p-1}\varphi(d),$$

de donde

$$\sum_{d|p-1}F(d)=\sum_{d|p-1}\varphi(d).$$

Veamos que $F(d)\leq\varphi(d)$, si d divide a $p-1$. Sea d un divisor de $p-1$.

Si $F(d)=0$, entonces $F(d)\leq\varphi(d)$.

Si $F(d)>0$, entonces existe a de orden d módulo p ($ord_p a=d$), por lo que los números $a,a^2,\ldots,a^d$ son incongruentes módulo p. Además ellos son raíces de x^d-1 módulo p, pues

$$(a^k)^d=(a^d)^k\equiv 1(mod\ p)$$

para todo valor entero positivo de k.

Por otra parte, x^d-1 tiene exactamente d soluciones incongruentes, por lo que $\{a,a^2,\ldots,a^d\}$ es un sistema completo de soluciones.

Ahora, si $(k,d)=1$, entonces es $ord_p a^k=d=ord_p a$. Además hay exactamente $\varphi(d)$ enteros $1\leq k\leq d$, tales que $(k,d)=1$. Entonces, si existe un número a de orden d módulo p, hay $\varphi(d)$ enteros de ese tipo menores que d.

De todo lo anterior se deduce para todo d divisor de $p-1$ que $F(d)\leq\varphi(d)$. Pero, como

$$\sum_{d|p-1}F(d)=\sum_{d|p-1}\varphi(d),$$

entonces para todo d divisor de $p-1$ tiene que ser $F(d)=\varphi(d)$, por lo que existen exactamente $\varphi(d)$ enteros de orden d módulo p incongruentes. **Q.e.d.**

Se puede concluir ahora el análisis demostrando la existencia de raíces primitivas para los números primos.

Corolario 4.1.4

Todo número primo p tiene raíces primitivas (exactamente $\varphi(p-1)$).

Demostración: Si p es primo, entonces hay $\varphi(p-1)$ enteros incongruentes de orden $p-1$ módulo p y cada uno de ellos es raíz primitiva. **Q.e.d.**

RAÍCES PRIMITIVAS DE POTENCIAS DE NÚMEROS PRIMOS

TEOREMA 4.1.8

Si p es un número primo impar con raíz primitiva r, entonces r o $r+p$ es raíz primitiva módulo p^2.

Demostración: Si r es raíz primitiva de p, entonces es $ord_p r = \varphi(p) = p-1$.

Sea $n = ord_{p^2} r$, entonces es $r^n \equiv 1(mod\ p^2)$; es decir $r^n \equiv 1(mod\ p)$, por lo que $p-1 = ord_p r$ divide a n.

Por otra parte, se conoce que $ord_n a$ divide a $\varphi(n)$, si $(a,n) = 1$, de modo que n divide a $\varphi(p^2) = p(p-1)$.

Resumiendo: se tiene que $n|p(p-1)$ y $(p-1)|n$. Entonces es $n = p-1$ o $n = p(p-1)$.

Ahora, si $n = p(p-1)$, entonces r es raíz primitiva módulo p^2 y se cumple el teorema.

Por otro lado, para $n = p-1$, es $r^{p-1} \equiv 1(mod\, p^2)$. Si $s = r+p$, entonces $s \equiv r(mod\, p)$ y por tanto, s es también raíz primitiva módulo p, de donde se deduce que

$$ord_{p^2} s = p-1 \quad \text{o} \quad ord_{p^2} s = p(p-1).$$

Pero

$$\begin{aligned} s^{p-1} &= (r+p)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} r^{p-1-k} p^k \\ &= r^{p-1} + (p-1)r^{p-2} + \binom{p-1}{2} r^{p-3} p^2 + \ldots + p^{p-1k} \\ &\equiv r^{p-1} + (p-1)r^{p-2} (mod\ p^2). \end{aligned}$$

Y como $ord_p s$ divide a $p-1$, se tiene que $s^{p-1} \equiv 1(mod\ p^2)$. Entonces es

$$s^{p-1} \equiv 1 + (p-1)r^{p-2} (mod\ p^2),$$

por lo que $s^{p-1} \not\equiv 1(mod\ p^2)$, pues en caso contrario sería $r^{p-2} \equiv 0(mod\ p^2)$, lo cual contradice el hecho de que p no divide a r.

Finalmente, de todo lo anterior se deduce que $ord_{p^2} s = p(p-1) = \varphi(p^2)$, por lo que $s = r+p$ es raíz primitiva de p^2. **Q.e.d.**

EJEMPLO: $r = 3$ es raíz primitiva de $p = 7$. Entonces es

$$ord_{49} 3 = 6 \qquad \text{o} \qquad ord_{49} 3 = 42.$$

Pero como $3^6 = 729 \equiv 43(mod\ 49)$, entonces es $ord_{49} 3 = 42 = \varphi(49)$. Luego $r = 3$ es también raíz primitiva de $p = 49$.

TEOREMA 4.1.9

Si p es un número primo impar, entonces p^k tiene raíz primitiva para todo entero positivo k. Más aún, si r es raíz primitiva módulo p^2, entonces r es raíz primitiva módulo p^k para todo entero positivo k.

Demostración: Del teorema anterior sabemos que p tiene raíz primitiva r, que lo es también de p^2, es decir, tal que $r^{p-1} \not\equiv 1 (mod\ p^2)$. Utilizaremos la inducción matemática (sobre k) para demostrar que para todo $k > 1$ es

$$r^{p^{k-2}(p-1)} \not\equiv 1 (mod\ p^k).$$

Habiendo demostrado esto se observa que si $n = ord_{p^2} r$, entonces se cumple que n divide a $\varphi(p^k) = p^{k-1}(p-1)$. Como $r^n \equiv 1 (mod\ p^k)$, entonces p divide a (p), quien a su vez divide a n, por lo que existe t $(0 \leq t \leq k-1)$, tal que $n = p^t(p-1)$.

Ahora, si $t \leq k-2$, entonces

$$r^{p^{k-2}(p-1)} = \left(r^{p^t(p-1)}\right)^{p(k-2-t)} \not\equiv 1 (mod\ p^k),$$

de donde $n = p^{k-1}(p-1)$, por lo que

$$ord_{p^k} r = p^{k-1}(p-1) = \varphi(p^k),$$

y por ello r es raíz primitiva módulo p^k.

Veamos entonces por inducción que para todo $k > 1$ es

$$r^{p^{k-2}(p-1)} \not\equiv 1 (mod\ p^k).$$

(1) Si $k = 2$, se conoce que $r^{p-1} \not\equiv 1 (mod\ p^2)$.

(2) Sea $r^{p^{k-2}(p-1)} \not\equiv 1 (mod\ p^k)$ para un valor de $k > 2$.

(3) Si $(r, p) = 1$, entonces $(r, p^{k-1}) = 1$ y el teorema de Euler asegura que

$$r^{p^{k-2}(p-1)} = r^{\varphi(p^{k-1}} \equiv 1 (mod\ p^{k-1}).$$

Entonces existe un entero d que no es divisible por p, tal que

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1}.$$

Al elevar a p se obtiene

$$\begin{aligned} r^{p^{k-1}(p-1)} &= (1 + dp^{k-1})^p = 1 + dp^{k-1} + \binom{p}{2}(dp^{k-1})^2 + \ldots + (dp^{k-1})^p \\ &\equiv 1 + dp^k (mod\ p^{k-1}), \end{aligned}$$

y como p no divide a d, se tiene que

$$r^{p^{k-2}(p-1)} \not\equiv 1 (mod\ p^k).$$

Q.e.d.

EJEMPLO: Se conoce que 3 es raíz primitiva módulo 7 y módulo $7^2 = 49$, entonces 3 es también raíz primitiva módulo 7^k para todo entero positivo k.

Hasta ahora se han estudiado las potencias de números primos impares ... ¿y las potencias de 2?

TEOREMA 4.1.10 *Sea a un número impar y $k \geq 3$ un entero. Entonces*

$$a^{\frac{\varphi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 (mod\ 2^k).$$

Demostración: (Por inducción). Sea $a = 2b + 1$

(1) Sea $k = 3$. Entonces es $a^2 = (2b+1)^2 = 4b(b+1)+1$. Pero $4b(b+1)$ es múltiplo de 8, por lo que $a^2 \equiv 1 (mod\ 8)$ y por ello es

$$a^{\frac{\varphi(2^2)}{2}} = a^2 \equiv 1 (mod\ 2^3).$$

(2) Sea $a^{2^{k-2}} \equiv 1 (mod\ 2^k)$.

(3) Entonces es $a^{2^{k-2}} = 1 + d2^k$, de donde, elevando al cuadrado, se tiene

$$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = (1 + d2^k)^2 = 1 + d2^{k-1} + d^2 2^{2k} \equiv 1 (mod\ 2^{k+1}).$$

Q.e.d.

Este teorema implica que entre las potencias de 2, 2 y 4 tienen raíz primitiva, pues si a es impar, entonces $ord_{2^k} a \neq \varphi(2^k)$. Por otra parte, el siguiente teorema confirmará que estas son las únicas potencias de 2 con raíz primitiva.

TEOREMA 4.1.11

Si $k \geq 3$, entonces es $ord_{2^k} 5 = \frac{\varphi(2^k)}{2} = 2^{k-2}$. Esto implica que para 2^k existe un elemento de mayor orden posible.

Demostración: Como 5 es impar, para $k \geq 3$ es $5^{2^{k-2}} \equiv 1 (mod\ 2^k)$, por lo que $ord_{2^k} 5$ divide a 2^{k-2}.

Veamos que 2^{k-2} divide a $ord_{2^k} 5$, de donde se deduce el teorema. Para ello demostraremos por inducción (sobre k) que

$$5^{2^{k-2}} \equiv 1 + 2^{k-1} \not\equiv 1 (mod\ 2^k).$$

(1) Para $k = 3$ es $5 = 1 + 4 \not\equiv 1 (mod\ 8)$.

(2) Sea $5^{2^{k-3}} \equiv 1 + 2^{k-1} (mod\ 2^k)$.

(3) Entonces para $k+1$ existe un entero positivo d, tal que

$$5^{2^{k-3}} = 1 + 2^{k-1} + d2^k,$$

de donde, elevando al cuadrado, se obtiene

$$\begin{aligned} 5^{2^{k-2}} &= \left(5^{2^{k-3}}\right)^2 = (1+2^{k-1})^2 + 2(1+2^{k-1})d2^k + d^2 2^{2k} \\ &\equiv (1+2^{k-1})^2 (mod\ 2^{k+1}) \\ &\equiv 1 + 2^k (mod\ 2^{k+1}). \end{aligned}$$

Entonces $5^{2^{k-2}} \equiv 1 + 2^{k-1} \not\equiv 1 (mod\ 2^k)$ y por ello 2^{k-3} divide a $ord_{2^k} 5$, quedando así demostrado el teorema. **Q.e.d.**

EN RESUMEN:

- Todas las potencias de números primos impares tienen raíz primitiva.
- Sólo las potencias 1 y 2 de 2 tienen raíz primitiva.

Resta estudiar cuáles enteros no son potencias de primos tienen raíz primitiva.

RAÍCES PRIMITIVAS DE ENTEROS COMPUESTOS

TEOREMA 4.1.12

Si n es un entero que no es potencia de un primo o 2 veces potencia de un primo, entonces n no tiene raíz primitiva.

Demostración: Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ la descomposición en factores primos de n y supongamos que r es raíz primitiva de n. Entonces es $(r, n) = 1$ y por ello $(r, p_k^{\alpha_k}) = 1$ para todo $k = 1, 2, \ldots, m$ y además es $ord_n r = \varphi(n)$.

El teorema de Euler garantiza que $r^{\varphi\left(p_k^{\alpha_k}\right)} \equiv 1 (mod\ p_k^{\alpha_k})$. Sea

$$U = \left[\varphi\left(p_1^{\alpha_1}\right), \varphi\left(p_2^{\alpha_2}\right), \ldots, \varphi\left(p_m^{\alpha_k m}\right)\right] \text{ (mínimo común múltiplo).}$$

Entonces $\varphi\left(p_k^{\alpha_k}\right)$ divide a U para todo $k = 1, 2, \ldots, m$ y por tanto es

$$r^U \equiv 1 (mod\ p_k^{\alpha_k}).$$

El teorema chino del resto implica entonces que $ord_n r = \varphi(n) \leq U$, pues r es raíz primitiva de n. Pero por las propiedades de φ es entonces

$$\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \varphi\left(p_2^{\alpha_2}\right) \cdots \varphi\left(p_m^{\alpha_k m}\right) \leq U,$$

con lo cual

$$\varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)\cdots\varphi\left(p_m^{\alpha_k m}\right) \leq \left[\varphi\left(p_1^{\alpha_1}\right),\varphi\left(p_2^{\alpha_2}\right),\ldots,\varphi\left(p_m^{\alpha_k m}\right)\right].$$

Esto sólo es válido (cumpliéndose la igualdad) si $\varphi\left(p_1^{\alpha_1}\right),\varphi\left(p_2^{\alpha_2}\right),\ldots,\varphi\left(p_m^{\alpha_k m}\right)$ son primos relativos 2 a 2.

Pero $\varphi(p^t)$ es par si p es impar o si $p_1 = 2$ y $\alpha_1 \geq 2$. Entonces $\varphi\left(p_1^{\alpha_1}\right),\varphi\left(p_2^{\alpha_2}\right),\ldots,\varphi\left(p_m^{\alpha_k m}\right)$ son primos relativos 2 a 2 cuando $p_1 = 2$ y $\alpha_1 \geq 2$ o cuando hay más de un factor primo, lo cual constituye una contradicción. **Q.e.d.**

Finalmente se considera el caso $n = 2p^\alpha$ con p primo impar.

Teorema 4.1.13

Sea p un número primo impar y $\alpha > 0$. Entonces $2p^\alpha$ tiene raíz primitiva. De hecho, si r es raíz primitiva módulo p^α, entonces

- *si r es impar, es raíz primitiva módulo $2p^\alpha$,*
- *si r es par, $r + p^\alpha$ es raíz primitiva módulo $2p^\alpha$.*

Demostración: Sea r raíz primitiva módulo p^α, entonces

$$r^{\varphi(p^\alpha)} \equiv 1(mod\ p^\alpha) \quad (y) \quad r^k \not\equiv 1(mod\ p^\alpha)\ \forall k < \varphi(p^\alpha).$$

Como $\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha)$, entonces

$$r^{2\varphi(p^\alpha)} \equiv 1(mod\ p^\alpha).$$

Sea r impar. Entonces $r^{2\varphi(p^\alpha)} \equiv 1(mod\ 2)$ y multiplicando es

$$r^{2\varphi(p^\alpha)} \equiv 1(mod\ 2p^\alpha).$$

Si fuera $r^k \equiv 1(mod\ 2p^\alpha)$ para $k < \varphi(2p^\alpha) = \varphi(p^\alpha)$, ello constituiría una contradicción con el hecho de que r es raíz primitiva módulo $2p^\alpha$.

Sea ahora r par. Entonces $r + p^\alpha$ es impar, por lo que

$$(r + p^\alpha)^{\varphi(2p^\alpha)} \equiv 1(mod\ 2) \quad (y) \quad (r + p^\alpha) \equiv (mod\ p^\alpha).$$

Entonces es

$$(r + p^\alpha)^{\varphi(2p^\alpha)} \equiv 1(mod\ p^\alpha)$$

y por tanto

$$(r + p^\alpha)^{\varphi(2p^\alpha)} \equiv 1(mod\ 2p^\alpha)$$

De manera análoga para $k < \varphi(2p^\alpha) = \varphi(p^\alpha)$ se comprueba que

$$(r + p^\alpha)^k \not\equiv 1 (mod\ 2p^\alpha).$$

Q.e.d.

EN RESUMEN:

Sólo tienen raíz primitiva los números de la forma p^α, 2, 4 y $2p^\alpha$ con p primo impar.

4.1.1. Ejercicios

1. Halle el orden de los enteros $2, 3$ y 5:
   a) módulo 17; b) módulo 19; c) módulo 23.

2. Demuestre las siguientes proposiciones:
   a) Si $ord_n a = hk$, entonces $ord_n a^h = k$.
   b) Si $ord_p a = 2k$, siendo p primo impar, entonces $a^k \equiv -1 (mod\ p)$.
   c) Si $ord_n a = n - 1$, entonces n es primo.

3. Si p es primo impar, demuestre que
   a) las únicas soluciones incongruentes de $x^2 \equiv 1 (mod\ p)$ son 1 y $p - 1$;
   b) la congruencia $x^p + \ldots + x^2 + x + 1 \equiv 0 (mod\ p)$ tiene exactamente $p - 2$ soluciones incongruentes que son $2, 3, \ldots, p - 1$.

4. Compruebe que cada una de las congruencias $x^2 \equiv 1 (mod\ 15)$, $x^2 \equiv -1 (mod\ 65)$ y $x^2 \equiv -2 (mod\ 33)$ tiene cuatro soluciones incongruentes; luego, el Teorema de Lagrange no vale en general cuando el módulo es un número compuesto.

5. Determine todas las raíces primitivas de los primos $p = 17, 19, 23$, expresando cada una como potencia de una de las raíces.

6. Partiendo de que 3 es raíz primitiva de 43, encuentre
   a) todos los enteros positivos menores que 43 que tienen orden 6 módulo 43;
   b) todos los enteros positivos menores que 43 que tienen orden 21 módulo 43.

7. Encuentre todos los enteros positivos menores que 61 que tienen orden 4 módulo 61.

8. *a*) Halle las cuatro raíces primitivas de 26 y las ocho raíces primitivas de 25.
   b) Determine todas las raíces primitivas de 32, 33 y 34.

4.2. Cálculo de índices

Se conoce que si r es raíz primitiva módulo m, entonces $1, r, r^2, \ldots, r^{\varphi(m)-1}$ es un sistema reducido de restos módulo m y por tanto, si $(a, m) = 1$ existe un único entero x $(0 \leq x \leq \varphi(m) - 1)$ tal que $r^x \equiv a(mod\ m)$.

Como se ha visto anteriormente, existe raíz primitiva módulo m para $m = 2, 4, p^\alpha, 2p^\alpha$ (para p primo $p \equiv 1(mod\ 2)$, $\alpha \geq 1$). Esto da pié a la siguiente definición.

DEFINICIÓN 4.2.1

Sea r una raíz primitiva módulo m y sea a un entero positivo con $(a, m) = 1$. Sea además μ el número del conjunto $\{0, 1, \ldots, \phi(m)-1\}$ unívocamente determinado por la congruencia

$$a \equiv r^\mu (mod\ m).$$

*Entonces μ se llama **índice de** a **respecto a la base** r **módulo** m y se denota por $\mu = ind_r a$ ó si no hay dudas por $\mu = ind\ a$.*

Nótese el parecido con el logaritmo. **Nótese** también que si $(a, m) = (b, m) = 1$ y $a \equiv b(mod\ m)$, entonces es $ind_r a = ind_r b$.

EJEMPLO: Se sabe que 3 es raíz primitiva módulo 7 y que $\varphi(7) = 6$, entonces

$$\begin{array}{ll} 3^0 \equiv 1(mod\ 7) \Rightarrow ind_3 1 = 0, & 3^1 \equiv 3(mod\ 7) \Rightarrow ind_3 3 = 1, \\ 3^2 \equiv 2(mod\ 7) \Rightarrow ind_3 2 = 2, & 3^3 \equiv 6(mod\ 7) \Rightarrow ind_3 6 = 3, \\ 3^4 \equiv 4(mod\ 7) \Rightarrow ind_3 4 = 4, & 3^5 \equiv 5(mod\ 7) \Rightarrow ind_3 5 = 5, \end{array}$$

Para el cálculo de índices se cumplen las siguientes relaciones:

TEOREMA 4.2.1

1. $ind_r(ab) \equiv ind_r a + ind_r b(mod\ \phi(m))$.
2. $ind_r(a^n) \equiv n \cdot ind_r a(mod\ \phi(m))$ *para* $n \geq 1$.
3. $ind_r 1 \equiv 0(mod\ \phi(m))$.
4. $ind_r r \equiv 1(mod\ \phi(m))$.
5. $ind_r(-1) \equiv \frac{\phi(m)}{2}(mod\ \phi(m))$ *para* $m > 2$.

Demostración: Obviamente (2) y (3) se derivan directamente de (1).

$$\begin{array}{rcl} a & \equiv & r^{ind_r a}(mod\ m), \\ b & \equiv & r^{ind_r b}(mod\ m), \end{array}$$

implican que

$$ab \equiv r^{ind_r a + ind_r b} (mod\ m).$$

Por otra parte es

$$ab \equiv r^{ind_r (ab)} (mod\ m),$$

de donde se deduce (1).

La afirmación (4) se infiere de

$$r \equiv r^{ind_r r} (mod\ m).$$

Para demostrar (5) se tiene en cuenta que $2|\phi(m)$ para todo $m > 2$ y se aplica el teorema de Fermat-Euler.

$$r^{\phi(m)} - 1 = \left(r^{\frac{\phi(m)}{2}} - 1\right)\left(r^{\frac{\phi(m)}{2}} + 1\right) \equiv 0 (mod\ m).$$

Si $m = 4$, entonces $r = 3$, de donde

$$3^{\frac{\phi(4)}{2}} + 1 = 4 \equiv 0 (mod\ 4).$$

Si $m = p^k$ con p primo impar, entonces no pueden ser ambos factores divisibles por p, puesto que tienen diferencia 2. Si r es raíz primitiva, entonces

$$r^{\frac{\phi(m)}{2}} \equiv -1 (mod\ m).$$

El caso $m = 2p^k$ para p primo impar se demuestra de modo análogo, teniendo en cuenta que r debe ser impar. **Q.e.d.**

Los índices son útiles en la resolución de cierto tipo de congruencias. Para los siguientes ejemplos se tendrá en cuenta que 3 es raíz primitiva módulo 17 y la siguiente tabla muestra los índices de enteros en base 3 módulo 17:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_3 a$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

CONGRUENCIAS LINEALES

$$ax \equiv b (mod\ m) \quad \text{con} \quad (a, m) = (b, m) = 1 \text{ (si } m \text{ tiene raíz primitiva } r).$$

Al aplicar el cálculo de índices se tiene

$$ind\ a + ind\ x \equiv ind\ b (mod\ \phi(m)),$$

de donde

$$ind\ x \equiv ind\ b - ind\ a (mod\ \phi(m)).$$

EJEMPLOS:

(1) Para $9x \equiv 7(mod\ 17)$ se tiene

$$ind_3 x \equiv ind_3 7 - ind_3 9 = 11 - 2 \equiv 9(mod\ 16).$$

Entonces es

$$x \equiv 14(mod\ 17).$$

(2) Para $6x^{12} \equiv 11(mod\ 17)$ es

$$12ind_3 x \equiv ind_3 11 - ind_3 6 = 7 - 15 = -8 \equiv 8(mod\ 16).$$

Al simplificar se obtiene

$$3ind_3 x \equiv 2(mod\ 4) \quad \Rightarrow \quad ind_3 x \equiv 2(mod\ 4);$$

es decir,

$$ind_3 x \equiv 2, 6, 10, 14(mod\ 16).$$

Entonces finalmente las soluciones son

$$x \equiv 9, 15, 8, 2(mod\ 17).$$

CONGRUENCIAS EXPONENCIALES

$a^x \equiv b(mod\ m)$ con $(a, m) = (b, m) = 1$ (si m tiene raíz primitiva r).

Al aplicar el cálculo de índices se tiene

$$x \cdot ind\ a \equiv ind\ b(mod\ \phi(m)),$$

que tiene solución cuando $(ind\ a, \phi(m))|ind\ b$.

EJEMPLO: Para $7^x \equiv 5(mod\ 17)$ se tiene

$$x \cdot ind_3 7 \equiv ind_3 5(mod\ 16),$$

es decir,

$$11x \equiv 5(mod\ 16),$$

de donde

$$x \equiv 15(mod\ 16).$$

4.2.1. Ejercicios

1. Determine el índice de 5 relativo a cada una de las raíces primitivas de 13.
2. Usando una tabla de índices para una raíz primitiva de 11, solucione las congruencias
   a) $7x^3 \equiv 3(mod\ 11)$
   b) $3x^4 \equiv 8(mod\ 11)$
   c) $x^8 \equiv 10(mod\ 11)$
3. La siguiente es una tabla de índices para el número primo 17 relativa la raíz primitiva 3:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

   Con la ayuda de la tabla resuelva las congruencias siguientes:
   a) $x^{12} \equiv 13(mod\ 17)$
   b) $8x^5 \equiv 10(mod\ 17)$
   c) $9x^8 \equiv 8(mod\ 17)$
   d) $7^x \equiv 7(mod\ 17)$
4. Halle el resto de la división de 3^{3^3} por 17. (Sugerencia: use la teoría de índices.)
5. Si r y r' son raíces primitivas del primo impar p, demuestre que para $(a, p) = 1$ se cumple
   $$ind_{r'} a \equiv (ind_r a)(ind_{r'} r)(mod\ p - 1).$$
   Esto se corresponde con la regla de cambio de base de los logaritmos.

4.3. Residuos de potencias

Se desea ahora obtener información respecto a la solubilidad de congruencias del tipo exponencial
$$ax^n \equiv b(mod\ m) \quad \text{para} \quad m \geq 2.$$
Nos limitaremos (sin perder generalidad) al caso $(a, m) = 1$.

Definición 4.3.1

Sean $m, n \in \mathbb{N}$ con $m, n \geq 2$ y $a \in \mathbb{Z}$ con $(a, m) = 1$. El número a se dice ***n-ésimo residuo de potencia módulo*** *m si la congruencia*
$$x^n \equiv a(mod\ m)$$
tiene solución.

Por el teorema de Fermat-Euler es

$$x^n \equiv ba^{\phi(m)-1}(mod\ m),$$

entonces, para solucionar congruencias polinomiales, de acuerdo al siguiente teorema, basta considerar residuos de potencias.

TEOREMA 4.3.1

Sea $f(x)$ un polinomio de coeficientes enteros. La cantidad de soluciones de

$$f(x) \equiv 0(mod\ m), \qquad m = \prod_{i=1}^{r} p_i^{\nu_i}$$

es $N = n_1 n_2 \cdots n_r$, donde los n_i $(i = 1, \ldots, r)$ representan la cantidad de soluciones de

$$f(x) \equiv 0(mod\ p_i^{\nu_i}).$$

Demostración: La ecuación $f(x) \equiv 0(mod\ m)$ es equivalente al sistema de ecuaciones en congruencias $f(x) \equiv 0(mod\ p_i^{\nu_i})$ para $i = 1, \ldots, r$. Sea (si existe) una solución $x_i \equiv c_i(mod\ p_i^{\nu_i})$ de la i-ésima congruencia. Entonces se tiene un sistema de congruencias que por el teorema chino del resto tiene solución única módulo m. Haciendo recorrer a c_i todas las soluciones incongruentes, se obtiene en total N soluciones de la congruencia original. **Q.e.d.**

TEOREMA 4.3.2

Sean m, n enteros positivos, tales que m tiene raíz primitiva r y sean $(a, m) = 1$ y $d = (n, \varphi(m))$. Entonces

$$x^n \equiv a(mod\ m)$$

tiene solución (exactamente d soluciones incongruentes) si y solo si $d|ind_r a$, lo cual es válido solo cuando

$$a^{\frac{\varphi(m)}{d}} \equiv 1(mod\ m).$$

Demostración: Al aplicar el cálculo de índices se tiene que

$$x^n \equiv a(mod\ m) \quad \Leftrightarrow \quad n \cdot ind_r x \equiv ind_r a(mod\ \varphi(m)).$$

Para $d = (n, \varphi(m))$, se conoce que la congruencia de la derecha tiene solución si y solo si $d|ind_r a$, en cuyo caso tiene exactamente d soluciones inconcruentes.

El teorema queda demostrado a partir de la relación

$$d|ind_r a \quad \Leftrightarrow \quad n\frac{\varphi(m)}{d} \cdot ind_r a = n\frac{ind_r a}{d} \cdot \varphi(m) \equiv 0(mod\ \varphi(m)),$$

pues

$$n\frac{\varphi(m)}{d}\cdot ind_r a \equiv 0(mod\ \varphi(m)) \quad \Leftrightarrow \quad a^{n\frac{\varphi(m)}{d}} \equiv 1(mod\ m)$$
$$\Leftrightarrow \quad a^{\frac{\varphi(m)}{d}} \equiv 1(mod\ m).$$

Q.e.d.

Veamos a continuación los diferentes casos particulares.

COROLARIO 4.3.1

Sea p un número primo impar con $p \nmid a$ y r una raíz primitiva módulo p^ν. Entonces

$$x^n \equiv a(mod\ p^\nu)$$

tiene exactamente $d = (n, p^{\nu-1}(p-1))$ soluciones incongruentes si $d|ind_r a$; es deir, si y sólo si se cumple la congruencia

$$a^{\frac{1}{d}p^{\nu-1}(p-1)} \equiv 1(mod\ p^\nu).$$

En otro caso no existe solución.

Demostración: En este caso es $\varphi(p^\nu) = p^{\nu-1}(p-1)$ y aplicando directamente el teorema anterior se obtiene la proposición. **Q.e.d.**

EJEMPLO: $x^3 \equiv a(mod\ p)$ con $p \geq 5$ y $(a, p) = 1$. Aquí es $d = (3, p-1)$. Luego, si $p \equiv -1(mod\ 6)$, la congruencia tiene una única solución. En cambio, si $p \equiv 1(mod\ 6)$, entonces la congruencia tiene tres soluciones o ninguna.

En general se cumple:

COROLARIO 4.3.2

Si el número natural $m > 1$ tiene raíces primitivas y $n|\phi(m)$, entonces la congruencia

$$x^n \equiv 1(mod\ m)$$

tiene exactamente n soluciones incongruentes módulo m.

Demostración: Usando el cálculo de índices es

$$n \cdot ind\ x \equiv ind\ 1 = 0(\quad \text{mód}\ \phi(m))$$

y se cumple $(n, \phi(m)) = t$, con el teorema 4.3.2 se concluye la demostración. **Q.e.d.**

COROLARIO 4.3.3

Sea p primo impar y sea $d = (n, p^{\nu-1}(p-1))$. Entonces existen exactamente $\frac{1}{d}p^{\nu-1}(p-1)$ residuos de potencia n-ésimos módulo p.

Demostración: Por el corolario 4.3.1 la cantidad de residuos de potencia coincide con la cantidad de soluciones de

$$a^{\frac{1}{d}p^{\nu-1}(p-1)} \equiv 1(\quad \text{mód } p^{\nu}).$$

El corolario anterior implica entonces la veracidad de esta proposición. **Q.e.d.**

EJEMPLO: $x^4 \equiv a(mod\ 17)$. Aquí es

$$d = (4, 16) = 4, \qquad \frac{1}{d}(p-1) = \frac{16}{4} = 4.$$

Entonces existen cuatro residuos bicuadráticos, que son $1, 4, 13, 16$.

Los siguientes teoremas se refieren a los módulos que son potencias de 2, para los cuales se conoce que no existen raíces primitivas. Veamos primeramente el siguiente lema.

Lema 4.3.1

El grupo de las clases primas de restos módulo 2^{ν} es para $\nu \geq 3$ producto directo de un grupo cíclico de orden 2 y un grupo cíclico de orden $2^{\nu-2}$. Todo elemento $\overline{a}$ del grupo se puede representar en la forma

$$\overline{a} = \overline{(-1)^r} \cdot \overline{5^s}, \qquad (r = 0, 1,\ s = 0, 1, \ldots, 2^{\nu-2} - 1).$$

Demostración: Es claro que $ord_{2^{\nu}}(-1) = 2$. Como

$$a^{2^{\nu-2}} \equiv 1(mod\ 2^{\nu}) \text{ y } \varphi(2^{\nu}) = 2^{\nu-1},$$

de

$$5^{2^{\nu-3}} = (1 + 2^2)^{2^{\nu-3}} \not\equiv 1(mod\ 2^{\nu})$$

se deduce que $ord_{2^{\nu}} 5 = 2^{\nu-2}$. De aquí que los números 5^s $(s = 0, \ldots, 2^{\nu-2} - 1)$ son incongruentes. La relación

$$\begin{aligned} 5^{s_1} &\equiv 1(mod\ 4) \\ -5^{s_2} &\equiv -1(mod\ 4) \end{aligned}$$

implica que $5^{s_1} \not\equiv -5^{s_2}(mod\ 2^{\nu})$. Entonces los $2^{\nu-1} = \phi(2^{\nu})$ números de la forma $(-1)^r 5^s$ forman un sistema reducido de restos módulo 2^{ν}, lo cual demuestra el lema. **Q.e.d.**

Teorema 4.3.3

Sea $a \equiv n \equiv 1(mod\ 2)$. Entonces la congruencia

$$x^n \equiv a(mod\ 2^{\nu}) \qquad (\nu \geq 1)$$

tiene solución única.

Demostración: En el caso $\nu = 1$ se observa que $x^n \equiv a(mod\ 2)$ tiene la solución $x \equiv 1(mod\ 2)$.

$\nu = 2$: En ese caso $x^n \equiv a(mod\ 4)$ tiene la solución

$$\begin{aligned} x &\equiv 1(mod\ 4) \quad \text{si} \quad a \equiv 1(mod\ 4) \\ x &\equiv -1(mod\ 4) \quad \text{si} \quad a \equiv -1(mod\ 4). \end{aligned}$$

$\nu \geq 3$: Por el lema 4.3.1 es

$$a \equiv (-1)^r 5^s (mod\ 2^\nu).$$

Hacemos

$$x \equiv (-1)^p 5^y (mod\ 2^\nu),$$

y sustituyendo es

$$(-1)^{np} 5^{ny} \equiv (-1)^r 5^s (mod\ 2^\nu).$$

Entonces $p \equiv r(mod\ 2)$ (considerándolo módulo 4) y $ny \equiv s(mod\ 2^{\nu-2})$, que tiene solución por ser $n \equiv 1(mod\ 2)$. Luego existe una única solución x módulo 2^ν. **Q.e.d.**

Teorema 4.3.4

Sea $a \equiv n \equiv 1(mod\ 2)$, $\nu \geq 1$ y $\alpha \geq 1$. Entonces la congruencia

$$x^{2^\alpha n} \equiv a(mod\ 2^\nu)$$

tiene para $\nu < \alpha + 2$ exactamente $2^{\nu-1}$ soluciones si $a \equiv 1(mod\ 2^\nu)$ y para $\nu \geq \alpha + 2$ tiene exactamente $2^{\alpha+1}$ soluciones si $a \equiv 1(mod\ 2^{\alpha+2})$. En otro caso no tiene solución.

Demostración: El caso $\nu = 1$ es trivial.

$\nu \geq 2$: Hacemos

$$a \equiv (-1)^r 5^s (mod\ 2^\nu), \qquad x \equiv (-1)^p 5^y (mod\ 2^\nu).$$

Entonces

$$5^{2^\alpha ny} \equiv 5^s (mod\ 2^\nu).$$

Considerando módulo 4 sólo puede ser $r \equiv 0(mod\ 2)$, por lo que la consideración $a \equiv 1(\ \text{mód}\ 4)$ es necesaria para la solubilidad de la congruencia. Entonces es $2^\alpha ny \equiv s(mod\ 2^{\nu-2})$.

CASO 1: $\nu < \alpha + 2$. La congruencia tiene solución si y sólo si $s = s'2^{\nu-2}$, es decir, $a \equiv 1(mod\ 2^\nu)$. Todos los $y \in \mathbb{Z}$ son solución, o sea, módulo $2^{\nu-2}$ hay $2^{\nu-2}$ soluciones y. p puede ser 0 ó 1. Luego, existen $2^{\nu-1}$ soluciones x de la congruencia.

CASO 2: $\nu \geq \alpha + 2$. La congruencia tiene solución si y sólo si $s = s'2^{\alpha}$, es decir, $a \equiv 1(mod\ 2^{\alpha+2})$. Entonces $ny \equiv s'(mod\ 2^{\nu-\alpha-2})$ tiene una única solución y módulo $2^{\nu-\alpha-2}$, por lo que hay 2^{α} soluciones y módulo $2^{\nu-2}$, p puede ser 0 ó 1. Luego, existen $2^{\alpha+1}$ soluciones x de la congruencia. **Q.e.d.**

A continuación se presenta una aplicación interesante del cálculo de índices.

TEST DE PRIMALIDAD

TEOREMA 4.3.5

Sea $m > 1$ un entero tal que existe un entero x con $x^{m-1} \equiv 1(mod\ m)$ y $x^{\frac{m-1}{q}} \not\equiv 1(mod\ m)$ para todo divisor primo q de $m-1$. Entonces m es primo.

Demostración: Si $x^{m-1} \equiv 1(mod\ m)$, entonces $ord_m x$ divide a $m-1$.

Supongamos que $ord_m x \neq m-1$, entonces existe $k > 1$ tal que $m - 1 = k \cdot ord_m x$. Sea q un divisor primo de k. Entonces

$$x^{\frac{m-1}{q}} = x^{\frac{k \cdot ord_m x}{q}} = (x^{ord_m x})^{\frac{k}{q}} \equiv 1(mod\ m),$$

lo cual contradice la hipótesis del teorema. Así es $ord_m x = m-1$. Pero como se cumple que $ord_m x \leq \varphi(m) \leq m-1$, entonces $\varphi(m) = m-1$ y por lo tanto, m es primo. **Q.e.d.**

EJEMPLO: Para $n = 1009$ se tiene que $11^{1008} \equiv 1(mod\ 1009)$ y $1008 = 2^4 \cdot 3^7 \cdot 7$. Además

$$\begin{aligned} 11^{\frac{1008}{2}} &= 11^{504} \equiv -1(mod\ 1009), \\ 11^{\frac{1008}{3}} &= 11^{336} \equiv 374(mod\ 1009), \\ 11^{\frac{1008}{7}} &= 11^{144} \equiv 935(mod\ 1009). \end{aligned}$$

Entonces 1009 es primo.

4.4. Congruencias cuadráticas

Sean $a, b, c, m \in \mathbb{Z}$ con $m \neq 1$ y $a \not\equiv 0(mod\ m)$. Se desea solucionar la congruencia

$$ax^2 + bx + c \equiv 0(mod\ m),$$

que, al multiplicar por $4a$ y completando cuadrados equivale a

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

DEFINICIÓN 4.4.1

Un entero a se dice ***residuo o resto cuadrático módulo*** *m, para $(a, m) = 1$, si es residuo de potencia 2 de m; es decir, si la ecuación $x^2 \equiv a(mod\ m)$ tiene solución.*

Surgen dos preguntas

- ¿Qué números son residuos cuadráticos o no-residuos cuadráticos para m dado?
- ¿Qué números m tienen la propiedad de que un a dado sea residuo cuadrático o no-residuo cuadrático?

Para estudiar este tema basta analizar la congruencia $x^2 \equiv a(mod\ p)$ para p primo, pues por el teorema 4.3.1 basta analizar la congruencia $x^2 \equiv a(mod\ p^\nu)$. Además se puede asumir $(a, p) = 1$, ya que si $p|a$, en el caso $\nu = 1$ se tendría $x \equiv 0(mod\ p)$, y para $\nu > 1$ se tiene que p divide a x, por lo que $x = py$, y como $p|a$ es $a = pa_1$ con $(p, a_1) = 1$; de modo que $py^2 \equiv a_1(mod\ p^{\nu-1})$.

Se consideran entonces las congruencias

$$x^2 \equiv a(mod\ p^\nu) \qquad \text{para} \qquad (a, p) = 1 \tag{4.1}$$

De las conclusiones a partir del teorema 4.3.2 se conoce para el caso $p = 2$ que:

1. $\nu = 1$: Existe una única solución.
2. $\nu = 2$:
   a) Si $a \equiv 1(mod\ 4)$, entonces existen exactamente 2 soluciones.
   b) Si $a \equiv -1(mod\ 4)$, entonces no hay solución.
3. $\nu \geq 3$:
   a) Si $a \equiv 1(mod\ 8)$, entonces existen exactamente 4 soluciones.
   b) Si $a \not\equiv 1(mod\ 8)$, entonces no hay solución.

TEOREMA 4.4.1

Sea p primo impar. Entonces la congruencia (4.1) tiene exactamente 2 soluciones o ninguna. Si a es residuo cuadrático módulo p también lo es módulo p^ν y viceversa.

Demostración: Es claro que $(2, p^{\nu-1}(p-1)) = 2$. Por el teorema 4.3.2 la congruencia (4.1) tiene exactamente 2 soluciones si $ind\ a \equiv 0(mod\ 2)$ y no tiene solución si $ind\ a \equiv 1(mod\ 2)$.

Resta comprobar que la paridad de $ind\ a$ no depende de ν. Sea r una raíz primitiva módulo p^ν ($\nu \geq 1$) y sea $\mu_\nu = ind_r a$ respecto al módulo p^ν. Entonces

$$a \equiv r^{\mu_\nu}(mod\ p^\nu) \quad \Rightarrow \quad a \equiv r^{\mu_\nu} \equiv r^{\mu_1}(mod\ p),$$

de donde

$$\mu_\nu \equiv \mu_1(mod\ p-1),$$

y por tanto es $\mu_\nu \equiv \mu_1(mod\ 2)$. **Q.e.d.**

A partir de ahora se considerará la congruencia (4.1) con $\nu = 1$. El teorema recién demostrado resultado más sencillo en este caso:

Teorema 4.4.2

Sea p primo impar. Entonces la congruencia $x^2 \equiv 2(mod\ p)$ tiene exactamente 2 soluciones o ninguna.

Demostración: x_0 es una solución de la congruencia $x^2 \equiv 2(mod\ p)$ es obvio que $-x_0$ también lo es. Como p es primo impar, entonces x_0 y $-x_0$ son incongruentes módulo p, con lo se tiene al menos dos soluciones de la ecuación $x^2 \equiv 2(mod\ p)$.

Veamos que no hay más soluciones. Sean x_1 una nueva solución de la congruencia original, de modo que

$$x_0^2 \equiv x_1^2 \equiv a(mod\ p).$$

Entonces

$$x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0(mod\ p),$$

de modo que $p|(x_0 - x_1)$ o $p|(x_0 + x_1)$, siendo así

$$x_1 \equiv x_0(mod\ p) \qquad \text{o} \qquad x_1 \equiv -x_0(mod\ p).$$

Q.e.d.

El teorema siguiente muestra la relación entre residuos y no-residuos cuadráticos y tiene una gran aplicación en la teoría.

Teorema 4.4.3

Sea p primo impar. Entonces existen tantos residuos cuadráticos como no-residuos cuadráticos. Los residuos cuadráticos están dados por

$$a \equiv 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 (mod\ p).$$

Demostración: Los números dados son incongruentes módulo p, pues si se cumple que $b^2 \equiv c^2 (mod\ p)$ con $1 \leq b, c \leq \frac{p-1}{2}$, entonces es

$$(b-c)(b+c) \equiv 0 (mod\ p).$$

Como $1 < b+c < p$, entonces es $b - c \equiv 0 (mod\ p)$, por lo que $b = c$.

Como $(p-k)^2 \equiv k^2 (mod\ p)$, entonces todo residuo cuadrático tiene que ser congruente a uno de los números a. **Q.e.d.**

El símbolo de Legendre[2], cuya definición se presenta a continuación, es una útil herramienta en la determinación de los residuos cuadráticos módulo p (primo impar).

DEFINICIÓN 4.4.2

Sea p primo impar y $p \nmid a$. El ***símbolo de Legendre*** $\left(\frac{a}{p}\right)$ *se define como*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si\ a\ es\ residuo\ cuadrático\ módulo\ p \\ -1 & si\ a\ es\ no\text{-}residuo\ cuadrático\ módulo\ p \end{cases}.$$

PROPIEDADES DEL SÍMBOLO DE LEGENDRE

Resulta sencillo comprobar que

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{b}{p}\right) \quad \text{para} \quad a \equiv b (mod\ p), \\ \left(\frac{a^2}{p}\right) &= 1. \end{aligned}$$

La primera igualdad es trivial. Por el teorema de Fermat-Euler es $a^{p-1} \equiv 1 (mod\ p)$, de donde $a^{\frac{p-1}{2}} \equiv \pm 1 (mod\ p)$. Por el teorema 4.3.2 $a^{\frac{p-1}{2}} \equiv 1 (mod\ p)$ si y sólo si $x^2 \equiv a (mod\ p)$ tiene solución.

De esto se deriva directamente la siguiente propiedad.

TEOREMA 4.4.4

Criterio de Euler

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\ p).$$

TEOREMA 4.4.5

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

[2] Adrien Marie Legendre (1752-1833)

Demostración:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (mod\ p).$$

Q.e.d.

TEOREMA 4.4.6

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{\frac{p-1}{2}}, \\ \left(\frac{2}{p}\right) &= (-1)^{\frac{p^2-1}{8}}. \end{aligned}$$

Demostración: La primera fórmula se deduce del teorema 4.4.4 con $a = -1$.

Sea

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

Si k es impar, sustituimos $-k$ módulo p por $p - k$. Entonces

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k k = 2 \cdot 4 \cdot 6 \cdots (p-1) = \left(\frac{p-1}{2}\right)! (-1)^{\frac{p^2-1}{8}}.$$

Pero $p \nmid \left(\frac{p-1}{2}\right)!$, por lo que

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} (mod\ p),$$

y por el criterio de Euler se obtiene la segunda fórmula. **Q.e.d.**

APLICACIONES DEL CRITERIO DE EULER

Analizar las siguientes ecuaciones en congruencias:

1. $x^2 \equiv -1 (mod\ p)$. Como

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 (mod\ 4) \\ -1 & p \equiv -1 (mod\ 4) \end{cases},$$

entonces la congruencia tiene solución para $p \equiv 1 (mod\ 4)$ y no la tiene para $p \equiv -1 (mod\ 4)$.

En el caso $p \equiv 1 (mod\ 4)$ las soluciones están dadas por

$$x \equiv \pm \left(\frac{p-1}{2}\right)! (mod\ p),$$

pues

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= (-1)(-2)\cdots\left(-\frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}} \\ &\equiv (p-1)(p-2)\cdots\left(p-\frac{p-1}{2}\right)(mod\ p),\end{aligned}$$

de donde (por el teorema de Wilson) se tiene

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

2. $x^2 \equiv a(mod\ p),\ \ p \equiv 3(mod\ 4),\ \ \left(\frac{a}{p}\right) = 1.$

   Las soluciones son

   $$x \equiv \pm a^{\frac{p+1}{4}}(mod\ p),$$

   pues

   $$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}}a \equiv \left(\frac{a}{p}\right)a \equiv a(mod\ p).$$

El criterio de Euler constituye un método para calcular $\left(\frac{a}{p}\right)$, pero resulta muy trabajoso para a grande.

El título de Lema no debe de ningún modo restar importancia al resultado siguiente de gran aplicación teórica.

TEOREMA 4.4.7 ***Lema de Gauss***

Sea p primo impar y $p \nmid a$. Se reducen los $\frac{p-1}{2}$ números

$$a, 2a, \ldots, \frac{p-1}{2}a$$

módulo p de manera que sus restos estén entre 1 y p. Sea μ la cantidad de restos mayores que $\frac{p}{2}$. Entonces

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Demostración: Sean los números

$$a, 2a, \ldots, \frac{p-1}{2}a$$

ya reducidos, distribuidos en los conjuntos

$$\begin{aligned}A &= \left\{a_1, a_2, \ldots, a_k;\ 0 < a_i < \frac{p}{2}\right\} \\ B &= \left\{b_1, b_2, \ldots, b_{\mu};\ \frac{p}{2} < a_i < p\right\}\end{aligned}$$

Como estos números son incongruentes módulo p, se tiene que $a_i \neq a_j$ y $b_i \neq b_j$ para $i \neq j$. Además se cumple que $k + \mu = \frac{p-1}{2}$.

Si fuera $a_i = p - b_j$, entonces existen x, y con $1 \leq x, y \leq \frac{p-1}{2}$ y $xa \equiv p - ya(mod\ p)$, es decir, $(x + y)a \equiv 0(mod\ p)$. Como $p \nmid a$, tiene que ser $x + y \equiv 0(mod\ p)$, lo que es imposible por ser $0 < x + y < p$. Entonces $a_i \neq p - b_j$.

Luego, es

$$A \cup \{p - b_1, p - b_2, \ldots, p - b_\mu\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\},$$

por lo que

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= \prod_{n=1}^{k} a_n \prod_{m=1}^{\mu} (p - b_m) \equiv (-1)^\mu \prod_{n=1}^{k} a_n \prod_{m=1}^{\mu} b_m (mod\ p) \\ &\equiv (-1)^\mu \prod_{r=1}^{\frac{p-1}{2}} (ra) \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} (mod\ p),\end{aligned}$$

y

$$(-1)^\mu \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (mod\ p).$$

Q.e.d.

Si se considera a μ módulo 2 se obtiene una forma simplificada del lema de Gauss, pues si $[x]$ representa a la parte entera de x y $p \nmid na$, entonces

$$na = \left[\frac{na}{p}\right] p + r_n \qquad 1 \leq r_n \leq p - 1.$$

De aquí se deduce

$$\begin{aligned}\sum_{n=1}^{\frac{p-1}{2}} na = \frac{p^2-1}{8} a &= \sum_{n=1}^{\frac{p-1}{2}} \left(\left[\frac{na}{p}\right] p + r_n\right) \\ &= p \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \sum_{n=1}^{k} a_n + \sum_{n=1}^{\mu} b_m,\end{aligned}$$

con a_n, b_m, k, μ como en el lema de Gauss. Entonces

$$\begin{aligned}\frac{p^2-1}{8} a &= p \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \sum_{n=1}^{k} a_n + \sum_{n=1}^{\mu} (p - b_m) - p\mu + 2 \sum_{n=1}^{\mu} b_m \\ &\equiv -\sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \frac{p^2-1}{8} + \mu (mod\ 2),\end{aligned}$$

es decir,

$$\mu \equiv \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \frac{p^2-1}{8}(a-1)(mod\ 2).$$

De aquí se tiene para $a = 2$ el teorema 4.4.6 en el caso $\left(\frac{2}{p}\right)$.

Para $a \equiv 1(mod\ 2)$ se obtiene el siguiente teorema.

TEOREMA 4.4.8 *Si a es impar, entonces*

$$\left(\frac{a}{p}\right) = (-1)^m \qquad con \qquad m = \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right].$$

El lema siguiente es básico para obtener la ley de reciprocidad cuadrática, una de las joyas de la corona de la reina de la Matemática. Su belleza ha ejercido siempre una extraña fascinación a los matemáticos. Euler planteó esta relación alrededor del 1750, pero no la demostró. Más tarde, en 1785, Legendre reformuló la relación a esta forma, pero tampoco la demostró totalmente. El primero en demostrarla (18 años después de conocida) fue Gauss y planteó 7 demostraciones diferentes. Luego se han realizado muchas demostraciones (hace relativamente pocos años ya se hablaba de la demostración 152).

LEMA 4.4.1 *Si $a \equiv b \equiv 1(mod\ 2)$ con $a, b \geq 3$ y $(a, b) = 1$, entonces*

$$\sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right] + \sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right] = \frac{a-1}{2} \cdot \frac{b-1}{2}.$$

Demostración: Consideremos los números $b_m - a_n$ con

$$m = 1, 2, \ldots, \frac{a-1}{2} \quad \text{y} \quad n = 1, 2, \ldots, \frac{b-1}{2}.$$

En total hay $\frac{a-1}{2}\frac{b-1}{2}$ números de ese tipo, lo que constituye el miembro derecho de la igualdad a demostrar.

La cantidad de números con $b_m - a_n = 0$ es 0, pues $(a, b) = 1$ implica que $m = at$ y $n = bt$, lo que es imposible.

La cantidad de números con $b_m - a_n > 0$ para m fijo está dada por $\left[\frac{bm}{a}\right]$. En total hay

$$\sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right].$$

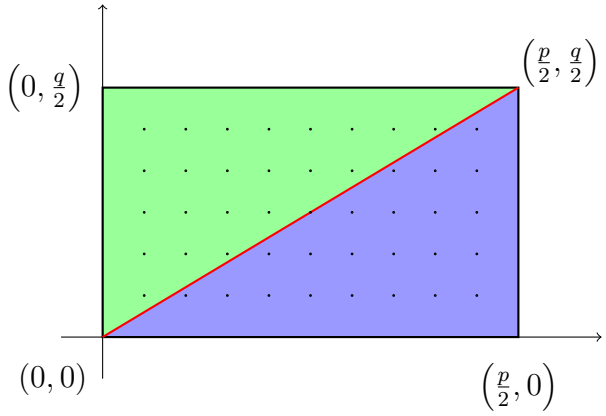
de esos números.

La cantidad de números con $b_m - a_n < 0$ para n fijo está dada por $\left[\frac{an}{b}\right]$. En total hay

$$\sum_{m=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right].$$

de esos números. **Q.e.d.**

Una demostración alternativa y muy visualizable de esta relación se obtiene al contar los nodos enteros en la figura siguiente, diferenciando los que se encuentran en cada triángulo y en la diagonal.



Teorema 4.4.9 ***Ley de reciprocidad cuadrática - Gauss***

Si p.q son números primos diferentes, entonces se cumple ***ley de reciprocidad cuadrática***

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

Demostración: Por el teorema 4.4.8 es

$$\left(\frac{q}{p}\right) = (-1)^{m_1} \quad \text{con} \quad m_1 = \sum_{n_1=1}^{\frac{p-1}{2}} \left[\frac{qn_1}{p}\right]$$

$$\left(\frac{p}{q}\right) = (-1)^{m_2} \quad \text{con} \quad m_2 = \sum_{n_2=1}^{\frac{q-1}{2}} \left[\frac{pn_2}{q}\right].$$

Del lema 4.4.1 se deduce entonces el teorema. **Q.e.d.**

RESUMEN

(A) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ para $a \equiv b(mod\ p)$.

(B) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(C) Ley de reciprocidad cuadrática: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$;

(D) Primer complemento de la ley de reciprocidad cuadrática: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

(E) Segundo complemento de la ley de reciprocidad cuadrática: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

EJEMPLOS:

1. ¿Es 74 residuo cuadrático módulo 131?

$$\begin{aligned}
(B) \quad &\Rightarrow \quad \left(\frac{74}{131}\right) = \left(\frac{2}{131}\right)\left(\frac{37}{131}\right) \\
(E) \quad &\Rightarrow \quad \left(\frac{2}{131}\right) = (-1)^{\frac{131^2-1}{8}} = -1 \\
(C) \quad &\Rightarrow \quad \left(\frac{37}{131}\right) = (-1)^{\frac{131-1}{2}\frac{37-1}{2}}\left(\frac{131}{7}\right) = \left(\frac{131}{37}\right) \\
(A) \text{ y } (B) \quad &\Rightarrow \quad \left(\frac{131}{37}\right) = \left(\frac{20}{37}\right) = \left(\frac{2^2}{37}\right)\left(\frac{5}{37}\right) = \left(\frac{5}{37}\right) \\
(C) \quad &\Rightarrow \quad \left(\frac{5}{37}\right) = (-1)^{\frac{5-1}{2}\frac{37-1}{2}}\left(\frac{37}{5}\right) = \left(\frac{37}{5}\right) \\
(A) \text{ y } (E) \quad &\Rightarrow \quad \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.
\end{aligned}$$

   Entonces $\left(\frac{74}{131}\right) = 1$, por lo que 74 es residuo cuadrático módulo 131.

2. ¿Para qué números primos p es 3 residuo o no-residuo cuadrático?

$$\begin{aligned}
(C) \quad &\Rightarrow \quad \left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) \\
p = 1 + 6k \quad &\Rightarrow \quad \left(\frac{3}{p}\right) = (-1)^k \\
p = -1 + 6k \quad &\Rightarrow \quad \left(\frac{3}{p}\right) = (-1)^{k+1}\left(-\frac{1}{3}\right) = (-1)^k.
\end{aligned}$$

   Entonces 3 es residuo cuadrático para $p \equiv \pm 1(mod\ 12)$ y es no-residuo cuadrático para $p \equiv \pm 5(mod\ 12)$.

4.4.1. Ejercicios

1. Halle todos los residuos cuadráticos de

   a) 3, b) 5, c) 13, d) 15, e) 18

2. Halle $\left(\frac{k}{3}\right)$ para $k = 1, 2, 3, 4$.

3. Calcule $\left(\frac{7}{11}\right)$ utilizando

   a) el criterio de Euler, b) el lema de Gauss.

4. Resuelva las siguientes congruencias cuadráticas:

   a) $x^2 + 7x + 10 \equiv 0 (mod\ 11)$;

   b) $3x^2 + 9x + 7 \equiv 0 (mod\ 13)$;

   c) $5x^2 + 6x + 1 \equiv 0 (mod\ 23)$.

5. *a)* Para p primo impar, demuestre que los residuos cuadráticos de p son congruentes módulo p a los enteros

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

   b) Compruebe que los residuos cuadráticos de 17 son $1, 2, 4, 8, 9, 13, 15, 16$.

6. Utilice el cálculo de índices para demostrar el criterio de Euler. (Sugerencia: vea el segundo teorema del capítulo anterior.)

7. Demuestre que 3 es residuo cuadrático de 23, pero es no-residuo de 19.

8. Use el lema de Gauss para calcular los siguientes símbolos de Legendre (es decir, en cada caso, halle el entero n para el que se cumple $\left(\frac{a}{p}\right) = (-1)^n$):

$$\text{a) } \left(\frac{8}{11}\right), \quad \text{b) } \left(\frac{7}{13}\right), \quad \text{c) } \left(\frac{5}{19}\right), \quad \text{d) } \left(\frac{11}{23}\right), \quad \text{e) } \left(\frac{6}{31}\right).$$

9. Si p es primo impar, demuestre que

$$\sum_{a=1}^{p-2} \frac{a(a+1)}{p} = -1.$$

   (Sugerencia: si a' es tal que $aa' \equiv 1 (mod\ p)$, entonces $\frac{a(a+1)}{p} = \frac{1+a'}{p}$; note que $1 + a'$ recorre un sistema completo de residuos módulo p, excepto para 1.)

10. Demuestre la siguientes proposiciones:

    a) Si p y $q = 2p + 1$ son primos impares, entonces -4 es raíz primitiva de q.

b) Si $p \equiv 1(mod\ 4)$ es primo, entonces -4 y $\frac{p-1}{4}$ son residuos cuadráticos de p.

11. Si $p \equiv 7(mod\ 8)$, demuestre que se cumple $p|2^{\frac{p-1}{2}} - 1$. (Sugerencia: utilice que $1 \equiv \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}(mod\ p)$.)

12. Use el problema 7 para comprobar que los números $2^n - 1$ son compuestos para $n = 11, 23, 83, 131, 179, 183, 239, 251$.

13. Considere la congruencia cuadrática $ax^2 + bx + c \equiv 0(mod\ p)$ con p primo que no divide al entero a y a, b, c enteros.

    a) Sea $p = 2$. Determine cuáles congruencias cuadráticas tienen solución.

    b) Sea p impar y sea $D = b^2 - ac$. Demuestre que la congruencia cuadrática es equivalente a la congruencia $y^2 \equiv D(mod\ p)$, siendo $y = 2ax + b$. Concluya de ello que si $D \equiv 0(mod\ p)$, entonces hay una única solución módulo p de la congruencia cuadrática; si D es residuo cuadrático módulo p, entonces hay dos soluciones incongruentes y si D es no residuo cuadrático, entonces no hay solución.

    c) Solucione
    (i) $x^2 + x + 1 \equiv 0(mod\ 7)$,
    (ii) $x^2 + 3x + 2 \equiv 0(mod\ 7)$,
    (iii) $x^2 + 2x - 2 \equiv 0(mod\ 7)$

14. Demuestre que si a es residuo cuadrático de p (primo), entonces la soluciones de $x^2 \equiv a(mod\ p)$ son

$$\begin{aligned} x &\equiv \pm a^{n+1}(mod\ p) \quad \text{si } p = 4n + 3 \\ x &\equiv \pm a^{n+1}(mod\ p) \text{ o } x \equiv \pm 2^{2n+1}a^{n+1}(mod\ p) \quad \text{si } p = 8n + 5. \end{aligned}$$

    a) si p = 4n +3. b) o si p = 8n +5.

15. Solucione

    a) $x^2 \equiv 1(mod\ 15)$, b) $x^2 \equiv 58(mod\ 77)$.

4.5. El maestro de todos los matemáticos

Fermat, aficionado a la Matemática y animador para sus conocidos matemáticos, debe haber sufrido su falta de habilidad para interesar a sus contemporáneos en la Teoría de Números. Un siglo tuvo que pasar hasta que un matemático de primera clase, Leonard Euler (1707-1783), apreciara su valor. Muchos de los teoremas presentados por Fermat fueron demostrados por Euler. Por su importancia le dedicaremos este espacio.

Hijo de un pastor luterano, en Basilea, Suiza. Comenzó los estudios de Teología a los 13 años en la Universidad de Basilea. Al conocer a Johann Bernoulli[3] -el primer matemático europeo- y entablar amistad con dos de sus hijos, Nicolaus[4] y Daniel[5], decidió dedicarse exclusivamente a la Matemática. Alcanzó su grado de Maestro en Ciencias en 1723 y en 1727, ganó un premio de la Academia de Ciencias de París por su primera publicación dedicada a la mejor ubicación de los mástiles de un barco.

Euler estuvo asociado en momentos diferentes a dos de las nuevas academias de su época, la Academia Imperial de San Petersburgo (de 1727 a 1741 y de 1766 a 1783) y la Real Academia de Berlín (de 1741 a 1766). En San Petersburgo conoció a Christian Goldbach (el de la famosa conjetura), un hombre que pasó de profesor Matemática a Ministro Ruso de Relaciones Exteriores. Parece ser que fue Goldbach uno de los más grandes interlocutores de Euler en la Teoría de Números.

Euler retornó a San Petersburgo en 1766 y pocos años tras su retorno quedó totalmente ciego. Pero la ceguera no redujo en modo alguno su trabajo científico y apoyado en una memoria fenomenal, sus escritos crecieron a tan enormes proporciones que se hicieron virtualmente inmanejables. Euler no solo es la figura clave del siglo XVIII de la Matemática, sino que es el más prolífico de todos los autores de obras matemáticas que han existido. Sus trabajos científicos, que se ha dedicado a publicar la Sociedad Suiza de Ciencias Naturales desde 1911, ocupan unos 87 gruesos volúmenes (no solo de Matemática) y tiene un promedio de unas 800 páginas escritas anualmente. Es de destacar además la calidad didáctica de sus trabajos, entre los que destaca en ese sentido el texto "Cartas a una princesa alemana" en tres volúmenes, escrito entre 178 y 1772.

En su despedida de duelo el marqués de Condorcet afirmó que cualquiera que se dedicase a la Matemática en el futuro sería

> "*guiado y sostenido por el genio de Euler [. . . pues . . .] "todos los matemáticos son sus discípulos.*".

Pero es a Laplace[6] a quien se debe la frase

> "*Leed a Euler, leed a Euler. El es el maestro de todos nosotros*".

[3]Johann Bernoulli (1667-1748)
[4]Nicolaus Bernoulli (1687-1759)
[5]Daniel Bernoulli (1700-1782)
[6]Pierre-Simon Laplace (1749-18279)

4.6. Ejercicios del capítulo

1. Determine todas las raíces primitivas módulo 17.

2. Resuelva las siguientes congruencias

   a) $45x \equiv 28(mod\ 17)$

   b) $x^7 \equiv 10(mod\ 17)$

   c) $13^x \equiv 16(mod\ 17)$

3. Calcule los símbolos de Legendre

$$\left(\frac{10}{13}\right), \quad \left(\frac{26}{59}\right), \quad \left(\frac{-209}{719}\right), \quad \left(\frac{3267}{5563}\right).$$

4. Resuelva (si es posible) las congruencias

   a) $3x^2 + 5x + 1 \equiv 0(mod\ 7)$

   b) $4x^2 + 2x + 3 \equiv 0(mod\ 15)$

   c) $x^2 - 3x + 2 \equiv 0(mod\ 6)$

   d) $3x^2 + 7x + 1 \equiv 0(mod\ 9)$

5. ¿Para qué números primos p $x^3 \equiv 1(mod\ p)$ tiene solución no trivial?

6. ¿Para qué números primos son residuos bicuadráticos los números 4 y -1?

7. *a*) Para un primo p de la forma $4k + 3$, demuestre que se cumple

$$\left(\frac{p-1}{2}\right)! \equiv 1(mod\ p) \qquad \text{ó} \qquad \left(\frac{p-1}{2}\right)! \equiv -1(mod\ p),$$

   por lo que $\left(\frac{p-1}{2}\right)!$ satisface la congruencia cuadrática $x^2 \equiv 1(mod\ p)$.

   b) Utilice el inciso a) para comprobar que si $p = 4k + 3$ es primo, entonces el producto de todos los enteros pares menores que p es incongruente módulo p a 1 o a -1 (Sugerencia: el Teorema de Fermat implica que $(2)^{\frac{p-1}{2}} \equiv \pm 1(mod\ p)$).

8. Halle dos soluciones de las congruencias cuadráticas $x^2 \equiv -1(mod\ 29)$ y $x^2 \equiv -1(mod\ 37)$.

9. Demuestre que si $p = 4k+3$ es primo y $a^2 + b^2 \equiv 0(mod\ p)$, entonces se cumple $a \equiv b \equiv 0(mod\ p)$. (Sugerencia: si $a \not\equiv 0(mod\ p)$, entonces existe un entero c tal que $ac \equiv 1(mod\ p)$, utilice este hecho para hallar una contradicción al teorema referido a congruencias cuadráticas.

10. Demuestre que $\phi(2^n - 1)$ es múltiplo de n para todo $n > 1$. (Sugerencia: $ord_{2^n-1}2 = n$.)

11. Sean $ord_n a = h$ y $ord_n b = k$. Demuestre que $ord_n ab | hk$. En particular, si $(h, k) = 1$, entonces $orden_n ab = hk$.

12. Si $ord_p a = 3$ con p primo impar, demuestre que $ord_p a + 1 = 6$. (Sugerencia: Como $a^2 + a + 1 \equiv 0(mod\ p)$, entonces se cumple que $(a + 1)^2 \equiv a(mod\ p)$ y $(a + 1)^3 \equiv -1(mod\ p)$.)

13. Demuestre las siguientes proposiciones:

    a) Los divisores primos impares del entero $n^2 + 1$ son de la forma $4k + 1$. (Sugerencia: $n^2 \equiv -1(mod\ p)$ para p primo impar implica que $4|\phi(p)$ por el teorema 4.3.2.)

    b) Los divisores primos impares del entero $n^4 + 1$ son de la forma $8k + 1$.

    c) Los divisores primos impares del entero $n^2 + n + 1$, que son diferentes de 3, son de la forma $6k + 1$.

14. Demuestre que existen infinitos primos de cada una de las formas $4k + 1$, $6k + 1$ y $8k + 1$. (Sugerencia: Asuma que solo hay finitos primos de la forma $4k + 1$ y denótelos por $p_1, \ldots, p_r$, considere al entero $(2p_1 \cdots p_r)^2 + 1$ y aplique el problema anterior.)

15. *a*) Demuestre que si p y q son primos impares y $q|a^p - 1$, entonces $q|a - 1$ ó $q = 2kp + 1$ para cierto entero k. (Sugerencia: Como $a^p \equiv 1(mod\ q)$, entonces $ord_q a = 1$ ó $ord_q a = p$; en el último caso $p|\phi(q)$.)

    b) Use el inciso a) para demostrar que si p es primo impar, entonces los divisores primos de $2^8 - 1$ son de la forma $2kp + 1$.

    c) Halle los menores divisores primos de $2^{17} - 1$ y $2^{29} - 1$.

16. Demuestre que existen infinitos primos de la forma $2kp + 1$ con p primo impar. (Sugerencia: Asuma que solo hay finitos primos de la forma $2kp + 1$, denótelos por $q_1, \ldots, q_r$ y considere al entero $(q_1 \cdots q_r)^2 - 1$.)

17. *a*) Compruebe que 2 is a raíz primitiva de 19, pero no de 17.

    b) Demuestre que 15 no tiene raíz primitiva calculando el orden de $2, 4, 7, 8, 11, 13$ y 14 módulo 15.

18. Sea r una raíz primitiva del entero n. Demuestre que r^k es raíz primitiva de n si y sólo si $(k, \phi(n)) = 1$.

19. *a*) Halle dos raíces primitivas de 10.

    b) Use que 3 es raíz primitiva de 17 para obtener las ocho raíces primitivas de 17.

20. Si r es una raíz primitiva del número primo p, demuestre las siguientes proposiciones:

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

    b) Si r' es otra raíz primitiva de p, entonces rr' no es raíz primitiva de p. (Sugerencia: por a), es $(rr')^{\frac{p-1}{2}} \equiv 1(mod\ p)$.)

    c) Si el entero r' cumple que $rr' \equiv 1(mod\ p)$, entonces r' es una raíz primitiva de p.

21. Para $p > 3$ primo, demuestre que las raíces primitivas de p ocurren en pares r, r', tales que $rr' \equiv 1(mod\ p)$. (Sugerencia: si r es una raíz primitiva de p, considere el entero $r' = r^{p-2}$.)

22. Sea r una raíz primitiva del número primo impar p. Demuestre que:

    a) Si $p \equiv 1(mod\ 4)$, entonces $-r$ es también raíz primitiva de p.

    b) Si $p \equiv 3(mod\ 4)$, entonces $ord_p(-r) = \frac{p-1}{2}$.

23. Presente una demostración diferente del teorema 3 de la sección 5, comprobando que si r una raíz primitiva del primo $p \equiv 1(mod\ 4)$, entonces $r^{\frac{p-1}{2}}$ satisface la congruencia cuadrática $x^2 + 1 \equiv 0(mod\ p)$.

24. Use que todo primo p tiene raíz primitiva para dar otra vía de demostración del Teorema de Wilson. (Sugerencia: si p tiene raíz primitiva r, entonces se cumple $(p-1)! \equiv r^{1+2+\ldots+(p-1)}(mod\ p)$.)

25. Si p es primo, demuestre que el producto de las $(p-1)$ raíces primitivas de p es congruente módulo p a $(-1)^{\phi(p-1)}$. (Sugerencia: si r una raíz primitiva de p, entonces r^k es raíz primitiva de p si $(k, p-1) = 1$; ahora use el teorema 7 de la sección 7.)

26. Para p primo impar, compruebe que

$$1^n + 2^n + \ldots + (p-1)^n \equiv \begin{cases} 0(mod\ p) & \text{si } (p-1) \nmid n \\ -1(mod\ p) & \text{si } (p-1) | n \end{cases}.$$

    (Sugerencia: Si $(p-1) \nmid n$ y r es una raíz primitiva de p, entonces

$$1 + r^n + r^{2n} + \ldots + r^{(p-2)n} = \frac{r^{(p-1)n} - 1}{r^n - 1}$$

    es congruente módulo p a la suma.)

27. Para p primo impar demuestre las siguientes proposiciones:

    a) Existen tantas raíces primitivas de $2p^n$ como de p^n.

b) Toda raíz primitiva r de p^n es también raíz primitiva de p. (Sugerencia: sea $ord_p r = k$; muestre que

$$r^{pk} \equiv 1(mod\ p^2), \ldots, r^{p^{n-1}k} \equiv 1(mod\ p^2),$$

por lo que $\phi(pn)|p^{n-1}k$.)

c) Una raíz primitiva de p^2 es también raíz primitiva de p^n para $n \geq 2$.

28. Si r es raíz primitiva de p^2, siendo p primo impar, demuestre que las soluciones de la congruencia $x^{p-1} \equiv 1(mod\ p^2)$ son precisamente los enteros $r^p, r^{2p}, \ldots, r^{p-1}p$.

29. *a*) Demuestre que 3 es raíz primitiva de todo entero de la forma 7^k y $2 \cdot 7^k$.

b) Halle una raíz primitiva de todo entero de la forma 17^k.

30. Obtenga todas las raíces primitivas de 41 y 82.

31. *a*) Demuestre que una raíz primitiva r de p^k con p primo impar es raíz primitiva de $2p^k$ si y sólo si r es impar.

b) Compruebe que $3, 33, 35$ y 39 son raíces primitivas de $578 = 2 \cdot 17^2$, pero 3^7 y 3^{11} no lo son.

32. Sea r una raíz primitiva del primo impar p y $(r+tp)^{p-1} \not\equiv 1(mod\ p^2)$. Demuestre que $r + tp$ es raíz primitiva de p^k para todo $k \geq 1$.

33. Si $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ es la ción prima de $n > 1$, se define el *exponente universal* $\lambda(n)$ de n como

$$\begin{aligned} \lambda(2) &= 1 \\ \lambda(2^2) &= 2 \\ \lambda(2^k) &= 2^{k-2} \quad \text{para } k \geq 3 \\ \lambda(n) &= \left[\lambda\left(2^{k_0}\right), \phi\left(p_1^{k_1}\right), \ldots, \phi\left(p_r^{k_r}\right)\right]. \end{aligned}$$

Demuestre las siguientes propiedades del exponente universal:

a) Para $n = 2, 4, p^k, 2p^k$ con p primo impar, se cumple $\lambda(n) = \phi(n)$.

b) Si $(a, 2^k) = 1$, entonces $a^{\lambda(2^k)} \equiv 1(mod\ 2^k)$. (Sugerencia: para $k \geq 3$, use inducción en k y el hecho de que $\lambda(2^{k+1}) = 2\lambda(2^k)$.)

c) Si $(a, n) = 1$, entonces $a^{\lambda(n)} \equiv 1(mod\ n)$. (Sugerencia: para cada potencia de primo p^k en la factorización de n se cumple $a^{\lambda(n)} \equiv 1(mod\ p^k)$.)

34. Compruebe que para $5040 = 2^4 3^2 5 \cdot 7$ se cumple

$$\lambda(5040) = 12 \qquad \text{y} \qquad \phi(5040) = 1152.$$

35. Use el problem 8 para demostrar que si $n \neq 2, 4, p^k, 2p^k$ con p primo impar, entonces n no tiene raíz primitiva. (Sugerencia: excepto para los casos $2, 4, p^k, 2p^k$, se tiene que $\lambda(n)|\frac{\phi(n)}{2}$; entonces $a^{\frac{\phi(n)}{2}} \equiv 1(mod\ n)$ siempre que $(a, n) = 1$.)

36. *a*) Demuestre que si $(a, n) = 1$, entonces la congruencia lineal $ax \equiv b(mod\ n)$ tiene la solución $x \equiv ba^{\lambda(n)-1}(mod\ n)$.

    b) Use el inciso a) para solucionar las congruencias $13x \equiv 2(mod\ 40)$ y $3x \equiv 13(mod\ 77)$.

37. *a*) Construya una tabla de índices para el número primo 17 respecto a la raíz primitiva 5. (Sugerencia: por el problema anterior es $ind_5 a \equiv 13 \cdot ind_3 a(mod\ 16)$.)

    b) Con la tabla del inciso a), resuelva las congruencias del problema 3.

38. Si r es una raíz primitiva del primo impar p, compruebe que

$$ind_r(-1) = ind_r(p-1) = \frac{p-1}{2}.$$

39. *a*) Determine los enteros a $(1 \leq a \leq 12)$ tal que $ax^4 \equiv b(mod\ 13)$ tiene solución para $b = 2, 5$ y 6.

    b) Determine los enteros a $(1 \leq a \leq p-1)$ tal que $x^4 \equiv a(mod\ p)$ tiene solución para $p = 7, 11$ y 13.

40. Utilice el último corolario para demostrar que si p es primo impar, entonces

    a) $x^2 \equiv -1(mod\ p)$ tiene solución si y sólo si $p \equiv 1(mod\ 4)$;

    b) $x^4 \equiv -1(mod\ p)$ tiene solución si y sólo si $p \equiv 1(mod\ 8)$.

41. Dada la congruencia $x^3 \equiv a(mod\ p)$, donde $p \geq 5$ es primo y $(a, p) = 1$, demuestre que

    a) Si $p \equiv 1(mod\ 6)$, entonces la congruencia o no tiene solución o tiene tres soluciones incongruentes módulo p;

    b) Si $p \equiv 5(mod\ 6)$, entonces la congruencia tiene solución única módulo p.

42. Demuestre que $x^3 \equiv 3(mod\ 19)$ no tiene solución, mientras que $x^3 \equiv 11(mod\ 19)$ tiene tres soluciones incongruentes.

43. Determine cuándo son solubles las congruencias

$$x^5 \equiv 13(mod\ 23) \qquad \text{y} \qquad x^7 \equiv 15(mod\ 29).$$

44. Si p es primo y $(k, p-1) = 1$, demuestre que los enteros

$$1^k, 2^k, 3^3, \ldots, (p-1)^k$$

forman un sistema reducido de restos módulo p..

45. Sea r una raíz primitiva del primo impar p y $d = (k, p-1)$. Demuestre que los valores de a para los que la congruencia $x^k \equiv a(mod\ p)$ tiene solución son

$$r^d, r^{2d}, \ldots, r^{\left[\frac{p-1}{d}\right]d}.$$

46. Si a es residuo cuadrático del primo impar p, demuestre que

    a) a no es raíz primitiva de p;

    b) $p - a$ es residuo cuadrático o no-residuo de p según sea $p \equiv 1(mod\ 4)$ ó $p \equiv 3(mod\ 4)$.

47. Si $p = 2k + 1$ es primo, demuestre que todo no-residuo cuadrático de p es raíz primitiva de p. (Sugerencia: Aplique el criterio de Euler.)

48. Si p es primo impar y $(a, p) = 1$,

    a) demuestre que la congruencia cuadrática $ax^2 + bx + c \equiv 0(mod\ p)$ tiene solución si y sólo si $b^2 - 4ac$ es cero o un residuo cuadrático de p.

    b) Use el inciso a) para comprobar que $5x^2 - 6x + 2 \equiv 0(mod\ 17)$ tiene solución.

49. *a*) Si $ab \equiv (mod\ p)$, donde r es residuo cuadrático del primo impar p, demuestre que a y b son simultáneamente residuos cuadráticos o no-residuos cuadráticos de p.

    b) Si a y b son simultáneamente residuos cuadráticos o no-residuos cuadráticos de p, demuestre que la congruencia $ax^2 = b(mod\ p)$ tiene solución. (Sugerencia: multiplique la congruencias dada por a', donde $aa' \equiv 1(mod\ p)$.)

50. Sea p primo impar y $(a, p) = (b, p) = 1$. Demuestre que las tres congruencias $x^2 \equiv a(mod\ p)$, $x^2 \equiv b(mod\ p)$, $x^2 \equiv ab(mod\ p)$ tienen solución ó exactamente una de ellas admite solución.

51. *a*) Conociendo que 2 es raíz primitiva de 19, halle todos los residuos cuadráticos de 19.

    b) Halle residuos cuadráticos de 29 y 31.

52. Si $n > 2$ y $(a, n) = 1$, entonces a es llamado *residuo cuadrático de* n si existe un entero x tal que $x^2 \equiv a(mod\ n)$. Demuestre que si a es residuo cuadrático de $n > 2$, entonces $a^{\frac{\phi(n)}{2}} \equiv 1(mod\ n)$.

53. Demuestre que el resultado del problema anterior no constituye una condición suficiente para la existencia de un residuo cuadrático de n; en otras palabras, encuentre enteros primos relativos a y n con $a^{\frac{\phi(n)}{2}} \equiv 1(mod\ n)$, para los cuales la congruencia $x^2 \equiv a(mod\ n)$ no tiene solución.

54. Dados p y $q = 4p + 1$ ambos primos, demuestre:

    a) Todo no-residuo cuadrático de q es una raíz primitiva de q o tiene orden 4 módulo q. (Sugerencia: si a es no-residuo cuadrático de q, entonces $-1 \equiv \left(\frac{a}{q}\right) \equiv a^{2p}(mod\ q)$, por lo que a tiene orden 1, 2, 4, p, $2p$ ó $4p$ módulo q.)

    b) El entero 2 es raíz primitiva de q.

55. Si r es raíz primitiva del primo impar p, demuestre que el producto de los residuos cuadráticos de p es congruente módulo p a $r^{\frac{p^2-1}{4}}$, mientras que el producto de los no-residuos cuadráticos de p es congruente módulo p a $r^{\frac{(p-1)^2}{4}}$. (Sugerencia: utilice el símbolo de Legendre.)

56. Demuestre que el producto de los residuos cuadráticos del primo impar p es congruente módulo p a 1 ó -1 según sea $p \equiv 3(mod\ 4)$ ó $p \equiv 1(mod\ 4)$. (Sugerencia: use el problema 7 y el hecho de que $r^{\frac{p-1}{1}} \equiv -1(mod\ p)$; o el problema 2a) de la sección 9.1 y la demostración del teorema 3, capítulo 5.)

57. *a*) Si $p > 3$ es primo, demuestre que p divide a la suma de sus residuos cuadráticos.

    b) Si $p > 5$ es primo, demuestre que p divide a la suma de los cuadrados de sus no-residuos cuadráticos.

58. Demuestre que para todo primo $p > 5$ existen enteros $1 \leq a, b \leq p-1$ tales que

$$\left(\frac{a}{p}\right) = \left(\frac{a+1}{p}\right) = 1 \qquad \text{y} \qquad \left(\frac{b}{p}\right) = \left(\frac{b+1}{p}\right) = 1.$$

    Es decir, hay residuos cuadráticos consecutivos de p y consecutive no-residuos consecutivos.

59. *a*) Sea p primo impar y $(a, p) = (k, p) = 1$. Demuestre que si la ecuación $x^2 - ay^2 = kp$ admite solución, entonces $\left(\frac{a}{p}\right) = 1$; por ejemplo, $\left(\frac{2}{7}\right) = 1$, pues $6^2 - 2 \cdot 2^2 = 4 \cdot 7$. (Sugerencia: si $x_0 y_0$ satisfacen la ecuación, entonces $(x_0 y_0^{p-2})^2 \equiv a(mod\ p)$.)

    b) Considerando la ecuación $x^2 + 5y^2 = 7$, demuestre que no necesariamente se cumple el recíproco del inciso a).

    c) Demuestre que para todo primo $p \equiv \pm 3(mod\ 8)$, la ecuación $x^2 - 2y^2 = p$ no tiene solución.

60. Si $p \equiv 1(mod\ 4)$, demuestre que

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = 0.$$

(Sugerencia: $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$.)

61. *a*) Demuestre que si p es un divisor primo de $839 = 38^2 - 5 \cdot 11^2$, entonces $\left(\frac{5}{p}\right) = 1$. Utilice ese hecho para comprobar que 839 es un número primo. (Sugerencia: basta considerar aquellos primos $p < 29$.)

b) Demuestre que $397 = 20^2 - 3$ y $733 = 29^2 - 3 \cdot 6^2$ son primos.

62. Resuelva la congruencia cuadrática $x^2 \equiv 11(mod\ 35)$. (Sugerencia: solucione $x^2 \equiv 11(mod\ 5)$ y $x^2 \equiv 11(mod\ 7)$ y utilice el teorema chino del resto.)

63. Compruebe que 7 es raíz primitiva de todo primo de la forma $p = 2^{4n} + 1$. (Sugerencia: como $p \equiv 3$ ó $5(mod\ 7)$, entonces $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = -1$.)

64. Sean a y $b > 1$ primos relativos, con b impar. Si $b = p_1 p_2 \cdots p_r$ es la descomposición de b en primos impares (no necesariamente diferentes), entonces el símbolo de Jacobi $\left(\frac{a}{b}\right)$ se define por

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right),$$

donde en el miembro derecho aparecen los símbolos de Legendre. Calcule los símbolos de Jacobi $\left(\frac{21}{221}\right)$, $\left(\frac{215}{253}\right)$ y $\left(\frac{631}{1099}\right)$.

65. Bajo la hipótesis del problema anterior, demuestre que si a es residuo cuadrático de b, entonces $\left(\frac{a}{b}\right) = 1$, pero el recíproco es falso.

66. Demuestre las siguientes propiedades del símbolo de Jacobi. Si b y b' son enteros positivos impares y $(aa', bb') = 1$, entonces se cumple:

a) $a \equiv a'(mod\ b)$ implica que $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$;

b) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$;

c) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$;

d) $\left(\frac{a^2}{b}\right) = \left(\frac{a}{b^2}\right) = 1$;

e) $\left(\frac{1}{b}\right) = 1$;

f) $\left(\frac{-1}{b}\right) = (-l)^{\frac{b-1}{2}}$; (Sugerencia: si u y v son números impares, entonces se cumple que $\frac{u-1}{2} + \frac{v-1}{2} \equiv \frac{uv-1}{2}(mod\ 2)$.)

g) $\left(\frac{2}{b}\right) = (-l)^{\frac{b^2-1}{8}}$; (Sugerencia: si u y v son números impares, entonces se cumple que $\frac{u^2-1}{8} + \frac{v^2-1}{8} \equiv \frac{(uv)^2-1}{8}(mod\ 2)$.)

67. Derive la ley de reciprocidad cuadrática generalizada: si a y b son enteros positivos primos relativos mayores que 1, entonces

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.$$

(Sugerencia: vea la sugerencia del problema 14f).]

68. Usando la ley de reciprocidad cuadrática generalizada, determine si la congruencia $x^2 \equiv 231(mod\ 1105)$ tiene solución.

69. *a)* Demuestre que 7 y 18 son las únicas soluciones incoongruentes de la ecuación $x \equiv -1(mod\ 5^2)$.

b) Use a) para hallar las soluciones de $x^2 \equiv -1(mod\ 5^3)$.

70. Solucione las siguientes congruencias cuadráticas:

a) $x^2 \equiv 7(mod\ 3^3)$.

b) $x^2 \equiv 14(mod\ 5^3)$.

c) $x^2 \equiv 2(mod\ 7^3)$.

71. Solucione la congruencia $x^2 \equiv 31(mod\ 11^4)$.

72. Encuentre las soluciones de $x^2 + 5x + 6 \equiv 0(mod\ 5^3)$ y $x^2 + x + 3 \equiv 0(mod\ 3^3)$.

73. Demuestre que si la congruencia $x^2 \equiv a(mod\ 2^n)$ con $n \geq 3$ tiene solución, entonces tiene exactamente cuatro soluciones incongruentes. (Sugerencia: si x_0 es una solución, entonces los enteros x_0, $-x_0$, $x_0 + 2^{n-1}$, $-x_0 + 2^{n-1}$ son incogruentes módulo $2n$ y cubren todas las soluciones.)

74. Partiendo de $23^2 \equiv 17(mod\ 2^7)$, halle otras tres soluciones de la congruencia $x^2 \equiv 17(mod\ 2^7)$.

75. Determine los valores de a para los que tiene solución las congruencias siguientes y halle la correspondiente solución:

a) $x^2 \equiv a(mod\ 2^4)$.

b) $x^2 \equiv a(mod\ 2^5)$.

c) $x^2 \equiv a(mod\ 2^6)$.

76. Para $n > 1$ fijo, muestre que todas las congruencias $x^2 \equiv a(mod\ n)$ que tienen solución, tienen igual cantidad de soluciones.

77. *a*) Sin hallarlas, determine el número de soluciones de las congruencias cuadráticas $x^2 \equiv 3(mod\ 11^4 23^2)$ y $x^2 \equiv 0(mod\ 2^3 3 \cdot 5^2)$.

    b) Resuelva la congruencia $x^2 \equiv 0(mod\ 2^3 3 \cdot 5^2)$.

78. *a*) Para un primo impar p, demuestre que la congruencia $2x^2 + 1 \equiv 0(mod\ p)$ tiene solución si y sólo si $p \equiv 1$ ó $3(mod\ 8)$.

    b) Resuelva la congruencia $2x^2 + 1 \equiv 0(mod\ 11^2)$. (Sugerencia: considere enteros de la forma $x_0 + 11k$, donde x_0 es una solución de la congruencia $2x^2 + 1 \equiv 0(mod\ 11)$.)

Capítulo 5

GRUPOS ABELIANOS FINITOS

5.1. Grupos abelianos finitos no isomorfos

Se conoce que si G es un grupo abeliano finito y $A_1, \ldots, A_r$ son subgrupos, entonces

$$G = A_1 \times A_2 \times \ldots \times A_r$$

es el producto directo, si para todo $g \in G$ existen únicos $a_i \in A_i$ para $i = 1, \ldots, r$ tal que $g = a_1 a_2 \cdots a_r$.

Los dos siguientes resultados (presentados sin demostración) son conocidos de los cursos de Álgebra.

TEOREMA 5.1.1 ***Teorema fundamental de grupos abelianos finitos***

Todo grupo abeliano finito es producto directo de grupos cíclicos de orden potencia de primo.

TEOREMA 5.1.2

La representación de un grupo abeliano finito de orden potencia de primo como producto directo de grupos cíclicos es única, excepto en el orden de los factores.

DEFINICIÓN 5.1.1

Se define la función aritmética $a(n)$ *como el* ***número de grupos abelianos de orden*** n ***no isomorfos***.

NÓTESE que la función $a(n)$ está definida para todo n natural.

Los teoremas 5.1.1 y 5.1.2 dan información sobre cómo hallar diferentes grupos de orden n. Para ello se descompone a n de algún modo como producto de potencias de números primos. Para cada descomposición de ese tipo existe un único grupo. Así,

para todo orden primo p existe un único grupo abeliano (cíclico de orden p). Luego, para $n = p^2$ existen dos grupos abelianos (cíclicos de orden p^2 y es producto directo de dos grupos cíclicos de orden p.

En general para $n = p^m$ existen tantos grupos abelianos como formas en que m se pueda representar en suma de números naturales (sin importar el orden de los sumandos).

En particular es

$$a(mn) = a(m)a(n) \qquad \text{si} \qquad (m,n) = 1.$$

Si $n = \prod_{i=1}^{r} p_i^{\nu_i}$ es la representación canónica de n, entonces

$$a(n) = \prod_{i=1}^{r} a\left(p_i^{\nu_i}\right).$$

DEFINICIÓN 5.1.2

Toda representación de un número natural n como suma de números naturales (sin importar el orden de los sumandos) se llama ***partición de*** *n. Se define la función aritmética $P(n)$ como el* ***número de particiones de*** *n.*

EJEMPLOS:

1. $n = 1$. Entonces $P(1) = 1$.
2. $n = 2$. Entonces se tienen las particiones $n = 2$, $n = 1 + 1$, de donde $P(2) = 2$.
3. $n = 3$. Entonces se tienen las particiones $n = 3$, $n = 2 + 1$, $n = 1 + 1 + 1$, de donde $P(3) = 3$.
4. $n = 4$. Entonces se tienen las particiones $n = 4$, $n = 3 + 1$, $n = 2 + 2$, $n = 2 + 1 + 1$, $n = 1 + 1 + 1 + 1$, de donde $P(4) = 5$.

Las siguientes tablas muestran los primeros valores de $P(n)$ y de $a(n)$ incluyendo en el último caso potencias de primos p.

n	1	2	3	4	5	6	7	8	9	10	11
$P(n)$	1	2	3	5	7	11	15	22	30	42	56

n	1	2	3	4	5	6	7	8	9	10	p	p^2	p^3	p^4	p^5
$a(n)$	1	1	1	2	1	1	1	3	2	1	1	2	3	5	7

Buscamos una acotación sencilla (aunque tosca) de $P(n)$. Para ello se tiene

- 1 partición $n = n$;
- $P(1)$ particiones que comienzan con $n - 1$;
- $P(2)$ particiones que comienzan con $n - 2$;
- ...
- $P(k)$ particiones que comienzan con $n - k$ para $k \leq n - k$;
- para $k > n - k$ se acota superiormente por $P(k)$.

Entonces

$$P(n) \leq 1 + \sum_{k=1}^{n-1} P(k). \tag{5.1}$$

Así se cumple que

$$P(n) \leq 2^{n-1}. \tag{5.2}$$

Demostración: (Inducción)

(i) Se cumple para $n = 1$, pues $P(1) = 1$.

(ii) Sea $P(k) \leq 2^{k-1}$ para $k \leq n - 1$

(iii) Entonces

$$P(n) \leq 1 + \sum_{k=1}^{n-1} P(k) \leq 1 + \sum_{k=1}^{n-1} 2^{k-1} \leq 1 + \sum_{k=0}^{n-2} 2^k = 1 + \frac{2^{n-1} - 1}{2 - 1} = 2^{n-1}.$$

Q.e.d.

Por otra parte, si $n = \prod_{i=1}^{r} p_i^{\nu_i}$ es la representación canónica de n, entonces

$$a(n) = \prod_{i=1}^{r} a\left(p_i^{\nu_i}\right) = \prod_{i=1}^{r} P(\nu_i). \tag{5.3}$$

De ello se deduce la acotación

$$a(n) \leq 2^{\nu_1 + \nu_2 + \ldots + \nu_r - r}. \tag{5.4}$$

DEFINICIÓN 5.1.3

Se definen ahora las funciones aritméticas

$\Omega(n)$: ***números de factores primos de*** n;

$\omega(n)$: ***números de factores primos diferentes de*** n.

NÓTESE que si $n = \prod_{i=1}^{r} p_i^{\nu_i}$ es la representación canónica de n, entonces

$$\Omega(n) = \sum_{i=1}^{r} \nu_i, \qquad \omega(n) = r.$$

TEOREMA 5.1.3

De 5.4 se deduce directamente que

$$a(n) \leq 2^{\Omega(n)-\omega(n)}.$$

Si n es libre de cuadrados, entonces

$$\Omega(n) = \omega(n),$$

y se tiene que $a(n) = 1$.

Si se considera la acotación

$$n = \prod_{i=1}^{r} p_i^{\nu_i} \geq 2^{\Omega(n)},$$

entonces, como $a(n) \leq 2^{\Omega(n)-\omega(n)} \leq n \cdot 2^{-\omega(n)}$, para $n > 1$ se tiene

$$a(n) \leq n \cdot 2^{-\omega(n)} \leq \frac{n}{2}.$$

5.2. Caracteres de grupos abelianos finitos

DEFINICIÓN 5.2.1

Un ***caracter*** χ *de un grupo abeliano finito G es una función*

$$\chi : G \to \mathbb{C},$$

no idénticamente nula, que cumple

$$\chi(ab) = \chi(a)\chi(b) \qquad \forall\ a, b \in G.$$

PROPIEDADES ELEMENTALES

1. Para todo $a \in G$ es $\chi(a) \neq 0$.

   Demostración: Supongamos que existe $c \in G$ con $\chi(c) = 0$. Entonces, si e es el elemento neutro de g, se tiene

   $$\chi(e) = \chi(c \cdot c^{-1}) = \chi(c)\chi(c^{-1}) = 0,$$

   de donde, para todo $a \in G$ es

   $$\chi(a) = \chi(ea) = \chi(e)\chi(a) = 0,$$

   lo cual es imposible. **Q.e.d.**

2. $\chi(e) = 1$.

   Demostración: Se deduce de

   $$\chi(e) = \chi(e^2) = \chi(e)\chi(e).$$

   Q.e.d.

3. Todo caracter es una raíz n-ésima de la unidad.

   Demostración: Todas las soluciones z_k de la ecuación $z^n - 1 = 0$ para $n \in N$ son las raíces n-ésimas de la unidad

   $$z_k = e^{2\pi i \frac{k}{n}}, \qquad k = 0, 1, \ldots, n-1.$$

   Si el grupo abeliano G es de orden n, entonces es $a^n = e$ para todo $a \in G$, de donde

   $$(\chi(a))^n = \chi(a^n) = \chi(e) = 1.$$

   Q.e.d.

El caracter χ_1 con $\chi_1(a) = 1$ para todo $a \in G$ se llama **caracter principal** de G.

TEOREMA 5.2.1

Un grupo abeliano de orden n tiene exactamente n caracteres diferentes.

Demostración:

Sea primeramente G un grupo cíclico, de modo que está conformado por las potencias

$$a, a^2, \ldots, a^n = e$$

de un elemento $a \in G$.

Sea χ un caracter de G. Entonces χ queda totalmente determinado por $\chi(a)$, pues $\chi(a^r) = (\chi(a))^r$.

Además, $\chi(a)$ es una raíz n-ésima de la unidad, pues

$$\chi(a^n) = \chi(e) = 1 = (\chi(a))^n .$$

Y como existen n raíces n-ésimas de la unidad, entonces existen n caracteres diferentes

Recíprocamente, toda raíz n-ésima de la unidad ρ define un caracter a través de $\chi(a) = \rho$, pues $a^{n_1}a^{n_2} = a^{n_3}$ implica que $n_1 + n_2 \equiv n_3 (mod\ n)$ y $\rho^{n_1}\rho^{n_2} = \rho^{n_3}$. Por tanto, existen exactamente n caracteres diferentes.

Sea ahora G un grupo abeliano finito cualquiera. Por el teorema 5.1.1 G es el producto directo de grupos cíclicos

$$G = G_1 \times G_2 \times \ldots \times G_k.$$

Si G_i tiene orden n_i para $i = 1, \ldots, k$, entonces G es de orden $n = n_1 n_2 \cdots n_k$. Sean a_i elementos generadores de G_i. Entonces todo $a \in G$ se expresa en modo único como

$$a = a_1^{r_1} a_2^{r_2} \cdots a_k^{r_k}, \qquad 0 \leq r_j \leq n_j - 1, \quad j = 1, \ldots, k.$$

Sea χ un caracter de G. Entonces

$$\chi(a) = (\chi(a_1))^{r_1} (\chi(a_2))^{r_2} \cdots (\chi(a_k))^{r_k} .$$

Sea ahora ρ_i una raíz n_i-ésima de la unidad. Entonces χ está unívocamente determinado por $\chi(a_i) = \rho_i$. Pero ρ_i puede tomar exactamente n_i valores diferentes, por lo que existen exactamente

$$n = n_1 n_2 \cdots n_k$$

caracteres diferentes de G. **Q.e.d.**

Denotemos por

$$\chi_1, \chi_2, \ldots, \chi_n$$

a los n caracteres diferentes de un grupo abeliano de orden n. Se define el **producto** de dos caracteres en la forma

$$(\chi_s \chi_t)(a) = \chi_s(a)\chi_t(a), \qquad a \in G.$$

Entonces $\chi_s\chi_t$ es también un caracter de G, pues

$$\begin{aligned} (\chi_s\chi_t)(ab) &= \chi_s(ab)\chi_t(ab) = \chi_s(a)\chi_s(b)\chi_t(a)\chi_t(b) \\ &= (\chi_s\chi_t)(a)(\chi_s\chi_t)(b). \end{aligned}$$

Así se cumple que:

Los caracteres de g conforman un grupo abeliano finito G^*, llamado *grupo de caracteres* de G, donde

- el caracter principal χ_1 es la unidad, y
- $\chi^{-1}(a) = \frac{1}{\chi(a)} = \overline{\chi(a)}$ (complejo conjugado).

TEOREMA 5.2.2

El grupo de caracteres G^* de un grupo abeliano finito G es isomorfo a G.

Demostración: Si G es de orden n, por el teorema 5.2.1 G^* es también de orden n. Sea

$$a = a_1^{r_1} a_2^{r_2} \cdots a_k^{r_k}, \qquad 0 \leq r_j \leq n_j - 1, \quad j = 1, \ldots, k$$

con

$$n = n_1 n_2 \cdots n_k$$

un representación básica de los elementos de G. Sea ρ_i una raíz primitiva n_i-ésima de la unidad, es decir,

$$\rho_i^{r_i} \neq 1 \quad (0 < r_i < n_i) \qquad \text{y} \qquad \rho_i^{n_i} = 1.$$

Entonces toda raíz n_i-ésima de la unidad se puede expresar en la forma $\rho_i^{s_i}$, con s_i determinado módulo n_i. Así es

$$\chi(a) = \rho_1^{r_1 s_1} \rho_2^{r_1 s_2} \cdots \rho_k^{r_k s_k},$$

por lo que a todo caracter $\chi \in G^*$ se le asigna biunívocamente un sistema de exponentes $s_1, s_2, \ldots, s_k$.

Obviamente la aplicación

$$\chi \mapsto a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k}$$

constituye un isomorfismo de G^* en G. **Q.e.d.**

TEOREMA 5.2.3

Sea

$$G = \{a_1, a_2, \ldots, a_n\}$$

un grupo abeliano finito de orden n y sea

$$G^* = \{\chi_1, \chi_2, \ldots, \chi_n\}$$

el correspondiente grupo de caracteres con caracter principal χ_1.

Entonces se cumple

$$\sum_{k=1}^{n} \chi_r(a_k) = \begin{cases} n & r = 1 \\ 0 & r > 1 \end{cases}, \tag{5.5}$$

$$\sum_{k=1}^{n} \chi_k(a_r) = \begin{cases} n & a_r = e \\ 0 & a_r \neq e \end{cases}. \tag{5.6}$$

Demostración:

(i) La expresión (5.5) es obvia para $r = 1$.

Si $r > 1$, existe $b \in G$ con $\chi_r(b) \neq 1$ y los elementos ba_k recorren todo G. Entonces

$$S_1 = \sum_{k=1}^{n} \chi_r(ba_k) = \sum_{k=1}^{n} \chi_r(b)\chi_r(a_k) = \chi_r(b)S_1,$$

de donde $S_1 = 0$.

(ii) La expresión (5.6) es obvia para $a_r = e$.

Si $a_r \neq e$, de modo análogo a (i), existe un caracter $\chi' \in G^*$ con $\chi'(a_r) \neq 1$. Ello es cierto, pues si

$$D = \det\left(\chi_i(a_j)\right)_{i,j=1}^{n}$$

(donde los índices i, j representan las filas y columnas respectivamente), entonces por (5.5) es $D\overline{D} = n^n$, por lo que $D \neq 0$, lo que implica que en D no existen dos columnas iguales. Así, en la columna r aparece a menos una vez $\chi(a_r) \neq 1$, pues $\chi(e) = 1$.

Entonces $\chi'\chi_k$ recorre a todo G^* y se tiene

$$S_2 = \sum_{k=1}^{n} \left(\chi'\chi_k\right)(a_r) = \sum_{k=1}^{n} \chi'(a_r)\chi_k(a_r) = \chi'(a_r)S_1,$$

de donde $S_2 = 0$. **Q.e.d.**

NOTA: Al sustituir en 5.5 a χ_r por $\chi_r\overline{\chi_s}$ y en 5.6 a a_r por $a_r a_s^{-1}$ se obtienen las

RELACIONES DE ORTOGONALIDAD

$$\sum_{k=1}^{n} \chi_r\overline{\chi_s}(a_k) = \begin{cases} n & r = s \\ 0 & r \neq s \end{cases}, \tag{5.7}$$

$$\sum_{k=1}^{n} \chi_k(a_r a_s^{-1}) = \begin{cases} n & r = s \\ 0 & r \neq s \end{cases}. \tag{5.8}$$

5.3. Caracteres de clases de restos

Sea G_m el grupo de las clases primas de restos módulo m. Entonces G_m es un grupo abeliano finito de orden $\phi(m)$. Los caracteres sobre G_m están definidos en las clases primas de restos

$$\overline{a} = \{x \in \mathbb{Z};\ x \equiv a(mod\ m)\}$$

con $(a, m) = 1$. Con el análisis siguiente se puede interpretar a los caracteres como funciones sobre $\mathbb{Z}$.

Sea $x \in \mathbb{Z}$. Si $(x, m) = 1$, se define

$$\chi(x) = \chi(\overline{a}) \qquad \text{para} \qquad x \in \overline{a}.$$

Note que esta definición es correcta, pues si $y \neq x$ con $y \in \overline{a}$, entonces $y \equiv a(mod\ m)$, de donde $y \equiv x(mod\ m)$, siendo así $(y, m) = (x, m) = 1$ y

$$\chi(y) = \chi(x).$$

Si $(x, m) > 1$, se define

$$\chi(x) = 0.$$

Definición 5.3.1

*Un **caracter de clases de restos módulo** m es una función definida en $\mathbb{Z}$ que cumple*

$$\begin{aligned} \chi(a) &= \chi(b) \qquad para \qquad a \equiv b(mod\ m), \\ \chi(ab) &= \chi(a)\chi(b) \qquad \forall\ a, b \in \mathbb{Z}, \\ \chi(a) &= 0 \qquad para \qquad (a, m) > 1, \\ \chi(a) &\neq 0 \qquad para \qquad (a, m) = 1. \end{aligned}$$

De lo estudiado en el epígrafe 5.2 se deduce que existen $\phi(m)$ caracteres de clases de restos módulo m, que conforman un grupo abeliano multiplicativo isomorfo al grupo de las clases primas de restos módulo m.

Aquí es χ_1 el caracter principal con $\chi_1(a) = 1$ para $(a, m) = 1$ y se cumple

$$\sum_{n\ mod\ m} \chi(n) = \begin{cases} \phi(m) & \chi = \chi_1 \\ 0 & \chi \neq \chi_1 \end{cases},$$

$$\sum_{\chi} \chi(n) = \begin{cases} \phi(m) & n \equiv 1(mod\ m) \\ 0 & n \not\equiv 1(mod\ m) \end{cases}.$$

La primera suma se desarrolla sobre cualquier sistema completo de restos módulo m, mientras que la segunda suma se toma sobre todos los caracteres de clases de restos.

Este concepto general de caracter de clases de restos se subordina al símbolo de Legendre $\left(\frac{a}{p}\right)$ estudiado en el capítulo anterior (definido para todo p primo impar y todo a con $(a,p)=1$). En efecto, si se considera además

$$\left(\frac{a}{p}\right)=0 \qquad \text{para} \qquad (a,p)>1,$$

entonces $\left(\frac{a}{p}\right)$ cumple las condiciones de la definición 5.3.1.

Como $\left(\frac{a}{p}\right)^2=1$ para $(a,p)=1$, se habla de **caracter cuadrático de clases de restos módulo** p. Por otra parte, de $\overline{\chi}=\chi^{-1}$ y $\chi^2=1$ se deduce que $\chi=\overline{\chi}$. De aquí que

Los caracteres cuadráticos de clases de restos módulo p están determinados por los caracteres reales diferentes del caracter principal.

EJEMPLO: Sea $m=5$. Entonces $\phi(5)=4$, por lo que existen 4 caracteres diferentes, cuyos valores posibles son $\pm1,\pm i$ para $(a,5)=1$. Aquí es

$$\chi(2)\chi(3)=\chi(6)=\chi(1)=1,$$

de donde

$$\chi(3)=(\chi(2))^{-1},$$

y

$$\chi(4)=(\chi(2))^2.$$

Entonces es

a	1	2	3	4	5
$\chi_1(a)$	1	1	1	1	0
$\chi_2(a)$	1	-1	-1	1	0
$\chi_3(a)$	1	i	$-i$	-1	0
$\chi_4(a)$	1	$-i$	i	-1	0

En particular es $\chi_2(a)=\left(\frac{a}{5}\right)$.

5.4. Sumas gaussianas

Las sumas gaussianas permiten relacionar los caracteres con las series numéricas.

DEFINICIÓN 5.4.1

Sea χ un caracter de clases de restos módulo m. Se define la ***suma gaussiana respecto a*** χ *como*

$$G(a,\chi)=\sum_{n \bmod m} \chi(n)e^{2\pi i\frac{an}{m}},$$

donde n recorre un sistema completo de restos módulo m. Se llama ***suma de Ramanujan*** *($c_m(a)$) a la suma gaussiana respecto al caracter principal χ_1, es decir*

$$c_m(a)=G(a,\chi_1)=\sum_{n=1,(n,m)=1}^{m} e^{2\pi i\frac{an}{m}}.$$

TEOREMA 5.4.1

Para $(m_1,m_2)=1$ se cumple

$$c_{m_1m_2}(a)=c_{m_1}(a)c_{m_2}(a).$$

Si p es primo y $\nu\geq 1$, entonces

$$c_{p^\nu}(a)=\begin{cases} p^{\nu-1}(p-1) & p^\nu|a \\ -p^{\nu-1} & -p^{\nu-1}|a \quad y \quad p^\nu\nmid a \\ 0 & -p^{\nu-1}\nmid a \end{cases}.$$

Demostración: Sea n_i que recorre un sistema completo de restos módulo m_i para $i=1,2$. Entonces $n_1m_2+n_2m_1$ recorre un sistema completo de restos módulo m_1m_2, pues $(m_1,m_2)=1$. Al sustituir se obtiene

$$c_{m_1}(a)c_{m_2}(a)=G(a,\chi_1)=\sum_{n_1=1,(n_1,m_1)=1}^{m_1} e^{2\pi i\frac{n_1m_2+n_2m_1}{m_1m_2}}=c_{m_1m_2}(a)$$

y

$$\begin{aligned} c_{p^\nu}(a) &= G(a,\chi_1)=\sum_{n=1,(n,p)=1}^{p^\nu} e^{2\pi ianp^{-\nu}} \\ &= \sum_{n=1}^{p^\nu} e^{2\pi ianp^{-\nu}}-\sum_{n=1,(n,p)>1}^{p^\nu} e^{2\pi ianp^{-\nu}}. \end{aligned}$$

Pero la segunda suma de la derecha se desarrolla para $p^{\nu-1}$ sumandos, para los cuales es $n=mp$, de modo que

$$c_{p^\nu}(a)=G(a,\chi_1)=\sum_{n=1}^{p^\nu} e^{2\pi ianp^{-\nu}}-\sum_{m=1}^{p^{\nu-1}} e^{2\pi iamp^{1-\nu}},$$

de donde se deduce la tesis del teorema **Q.e.d.**

TEOREMA 5.4.2

Para cualesquiera caracteres de clases de restos χ módulo m y para $(a,m)=1$ se cumple

$$G(a,\chi)=\overline{\chi(a)}G(1,\chi).$$

Demostración: Como $(a,m)=1$, junto con n los números an recorren un sistema completo de restos módulo m. Como $\chi(a)\overline{\chi(a)}=1$, se tiene

$$\chi(n)=\chi(a)\overline{\chi(a)}\chi(n)=\overline{\chi(a)}\chi(an).$$

Entonces

$$\begin{aligned} G(a,\chi) &= \sum_{n \bmod m} \chi(n)e^{2\pi i\frac{an}{m}}=\overline{\chi(a)}\sum_{n \bmod m}\chi(an)e^{2\pi i\frac{an}{m}} \\ &= \overline{\chi(a)}\sum_{k \bmod m}\chi(k)e^{2\pi i\frac{k}{m}} \\ &= \overline{\chi(a)}G(1,\chi). \end{aligned}$$

Q.e.d.

Si $(a,m)>1$, entonces es $\chi(a)=0$, pero $G(a,\chi)$ puede ser no nulo.

TEOREMA 5.4.3

Sea χ un caracter de clases de restos módulo m y sea $a\in\mathbb{Z}$ con $(a,m)>1$ tal que $G(a,\chi)\neq 0$. Entonces existe un divisor t de m con $0<t<m$ tal que

$$\chi(b)=1 \quad para \quad (b,m)=1 \quad y \quad b\equiv 1(mod\ t).$$

Demostración: Sean $(a,m)=d$ y $t=\frac{m}{d}$. Como $d>1$ es $0<t<m$. Sea ahora b tal que $(b,m)=1$ y $b\equiv 1(mod\ t)$. Entonces

$$\begin{aligned} G(a,\chi) &= \sum_{n \bmod m} \chi(n)e^{2\pi i\frac{an}{m}}=\overline{\chi(a)}\sum_{n \bmod m}\chi(bn)e^{2\pi i\frac{abn}{m}} \\ &= \chi(b)\sum_{n \bmod m}\chi(n)e^{2\pi i\frac{abn}{m}}. \end{aligned}$$

Pero

$$abn=an+antk=an+\frac{a}{b}nmk\equiv an(mod\ m),$$

de donde

$$G(a,\chi)=\chi(b)\sum_{n \bmod m}\chi(n)e^{2\pi i\frac{an}{m}}=\chi(b)G(a,\chi),$$

por lo que $\chi(b)=1$, ya que $G(a,\chi)\neq 0$. **Q.e.d.**

DEFINICIÓN 5.4.2

Un caracter χ de clases de restos módulo m se dice ***primitivo*** *si para todo $t|m$ existe $b \in \mathbb{Z}$ con $(b,m)=1$ y $b \equiv 1(mod\ t)$, tal que $\chi(b) \neq 1$.*

Para $m > 1$ el caracter principal χ_1 no es primitivo, pues para todo b con $(b,m)=1$ es $\chi(b)=1$.

Para $m = p$ es primo, entonces todo caracter $\chi \neq \chi_1$ es primitivo, pues el único divisor posible de de p menor que p es $t=1$. Si χ no fuera primitivo, sería $\chi(b)=1$ para todo b con $(b,p)=1$, lo cual sólo es válido para el caracter principal.

TEOREMA 5.4.4

Sea χ un caracter primitivo de clases de restos módulo m. Entonces $G(a,\chi)=0$ para todo $a \in \mathbb{Z}$ con $(a,m)=1$.

Demostración: Negación del teorema 5.4.3. **Q.e.d.**

TEOREMA 5.4.5

Sea χ un caracter primitivo de clases de restos módulo m. Entonces

$$|G(1,\chi)| = \sqrt{m}.$$

Demostración:

$$\begin{aligned} |G(1,\chi)|^2 &= G(1,\chi)\overline{G(1,\chi)} = G(1,\chi)\sum_{n=1}^{m}\overline{\chi(n)}e^{-2\pi i\frac{n}{m}} \\ &= \sum_{n=1}^{m} G(n,\chi)e^{-2\pi i\frac{n}{m}} = \sum_{n=1}^{m}\sum_{k=1}^{m}\chi(k)e^{2\pi i\frac{n(k-1)}{m}} \\ &= \sum_{k=1}^{m}\chi(k)\sum_{n=1}^{m}e^{2\pi i\frac{n(k-1)}{m}} = m\chi(1) = m. \end{aligned}$$

Q.e.d.

Consideremos ahora el caracter cuadrático de clases de restos respecto a un número primo impar p

$$\chi(a) = \left(\frac{a}{p}\right).$$

Entonces es

$$G(a,\chi) = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)e^{2\pi i\frac{an}{p}},$$

y del teorema 5.4.2 se deduce

$$G(a,\chi) = \left(\frac{a}{p}\right)G(1,\chi).$$

TEOREMA 5.4.6

Sea p primo impar y $\chi(n) = \left(\frac{n}{p}\right)$. Entonces se cumple

$$(G(1,\chi))^2 = (-1)^{\frac{p-1}{2}} p. \tag{5.9}$$

Demostración: Aquí es

$$(G(1,\chi))^2 = \sum_{n=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{n}{p}\right)\left(\frac{k}{p}\right)e^{2\pi i\frac{n+k}{m}}.$$

Para n fijo se cumple que para todo k existe m con $(m,p)=1$ determinado unívocamente a través de $k \equiv nm(mod\ p)$. Entonces

$$\begin{aligned} G(1,\chi)^2 &= \sum_{n=1}^{p-1}\sum_{m=1}^{p-1}\left(\frac{n^2m}{p}\right)e^{2\pi i\frac{n(m+1)}{p}} \\ &= \sum_{m=1}^{p-1}\left(\frac{m}{p}\right)\sum_{n=1}^{p-1}e^{2\pi i\frac{n(m+1)}{p}}. \end{aligned}$$

La segunda suma es $c_p(m+1)$ que vale 1 o -1 según sea $p|(m+1)$ o $p\nmid(m+1)$ respectivamente, por lo que

$$\begin{aligned} G(1,\chi)^2 &= -\sum_{m=1}^{p-2}\left(\frac{m}{p}\right) + (p-1)\left(\frac{-1}{p}\right) \\ &= -\sum_{m=1}^{p-1}\left(\frac{m}{p}\right) + p\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}p, \end{aligned}$$

por los teoremas 4.4.3 y 4.4.6. **Q.e.d.**

Entonces para calcular $G(1,\chi)$ para $\chi(n) = \left(\frac{n}{p}\right)$, según 5.9, "solo" resta determinar el signo en

$$G(1,\chi) = \pm\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Pero precisamente en ello radica la gran dificultad, lo cual se verá en el siguiente epígrafe.

Para primos impares p es

$$G(a,\chi) = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)e^{2\pi i\frac{ak}{p}} = \sum_r e^{2\pi i\frac{ar}{p}} - \sum_n e^{2\pi i\frac{an}{p}},$$

donde las sumas del miembro derecho se desarrollan respectivamente sobre los residuos cuadráticos r y sobre los no-residuos cuadráticos n. Pero

$$1 + \sum_r e^{2\pi i\frac{ar}{p}} + \sum_n e^{2\pi i\frac{an}{p}} = \sum_{k=0}^{p-1} e^{2\pi i\frac{ak}{p}} = 0$$

para $(a,p)=1$, de donde

$$G(a,\chi)=1+2\sum_{r} e^{2\pi i\frac{ar}{p}}.$$

Como toda congruencia $x^2\equiv r(mod\ p)$ tiene exactamente dos soluciones dadas por $x\equiv\pm k(mod\ p)$, entonces

$$G(a,\chi)=\sum_{k=0}^{p-1} e^{2\pi i\frac{a}{p}k^2}. \tag{5.10}$$

5.5. La ley de reciprocidad cuadrática a la luz de las sumas gaussianas

DEFINICIÓN 5.5.1

Sean $a\in\mathbb{N}$ y $b\in\mathbb{Z}$ con $(a,b)=1$. La suma

$$G_a(b)=\sum_{n=0}^{a-1} e^{2\pi i\frac{b}{a}n^2}$$

*se llama **suma gaussiana cuadrática respecto a** a.*

Primeramente se demostrará que la suma gaussiana cuadrática respecto a a cumple una propiedad multiplicativa. Con ello nos limitaremos al caso $a=p^\nu$. Así, para $p=2$ se calcula directamente $G_a(b)$. Para $p\neq 2^\nu$ se calcula primero $G_a(1)$ y luego se halla $G_a(b)$ recursivamente a partir de una ley de reciprocidad.

TEOREMA 5.5.1

$$(a,a')=1 \qquad \Rightarrow \qquad G_a(a'b)G_{a'}(ab)=G_{aa'}(b).$$

Demostración:

$$\begin{aligned} G_a(a'b)G_{a'}(ab) &= \sum_{n=0}^{a-1}\sum_{n'=0}^{b-1} e^{2\pi i\frac{b}{aa'}(a'^2n^2+a^2n'^2)} \\ &= \sum_{n=0}^{a-1}\sum_{n'=0}^{b-1} e^{2\pi i\frac{b}{aa'}(a'n+an')^2} \\ &= \sum_{k=0}^{aa'-1} e^{2\pi i\frac{b}{aa'}k^2}=G_{aa'}(b). \end{aligned}$$

Aquí se usó que $a'n+an'$ recorre un sistema completo de restos módulo nn' y que

$$\sum_{n=0}^{a-1}\sum_{n'=0}^{b-1} e^{2\pi ibnn'}=0.$$

Q.e.d.

TEOREMA 5.5.2

Si $b \equiv 1(mod\ 2)$, *entonces*

$$G_2(b) = 0 \tag{5.11}$$

y para $\nu > 1$ *es*

$$G_{2^\nu}(b) = \begin{cases} 2^{\frac{\nu}{2}}(1+i^b) & para\ \nu \equiv 0(mod\ 2) \\ 2^{\frac{\nu+1}{2}} e^{\pi i \frac{b}{4}} & para\ \nu \equiv 1(mod\ 2) \end{cases}. \tag{5.12}$$

Demostración: Para $\nu = 1$ es

$$G_2(b) = e^0 + e^{\pi i b} = 1 - 1 = 0$$

para b impar, lo que demuestra (5.11)

Para $\nu = 2$ y $\nu = 3$ una cálculo análogo demuestra (5.12).

Para $\nu > 3$ es

$$\begin{aligned} G_{2^\nu}(b) &= \sum_{n=0}^{2^{\nu-2}-1} \sum_{r=0}^{3} e^{2\pi i b 2^{-\nu}(n+2^{\nu-2}r)^2} \\ &= \sum_{n=0}^{2^{\nu-2}-1} e^{2\pi i b 2^{-\nu} n^2} \sum_{r=0}^{3} e^{\pi i b n r} \\ &= 4 \sum_{m=0}^{2^{\nu-2}-1} e^{2\pi i b 2^{2-\nu} m^2}. \end{aligned}$$

Aquí se usó que

$$\sum_{r=0}^{3} e^{\pi i b n r} = \begin{cases} 0 & n \text{ impar} \\ 4 & n = 4m \end{cases}.$$

Pero

$$(m + 2^{\nu-3})^2 \equiv m^2 (mod\ 2^{\nu-2}) \quad \text{para} \quad \nu > 3,$$

de donde

$$G_{2^\nu}(b) = 2 \sum_{m=0}^{2^{\nu-2}-1} e^{2\pi i b 2^{2-\nu} m^2} = 2 G_{2^{\nu-2}}(b).$$

Con ello $G_{2^\nu}(b)$ se reduce a $G_4(b)$ ó $G_8(b)$, según sea ν par o impar. **Q.e.d.**

TEOREMA 5.5.3

$$(a,b) = 1 \qquad \Rightarrow \qquad |G_a(b)| = \begin{cases} \sqrt{a} & para\ a \equiv 1(mod\ 2) \\ \sqrt{2a} & para\ a \equiv 0(mod\ 4) \\ 0 & para\ a \equiv 2(mod\ 4) \end{cases}. \tag{5.13}$$

Demostración:

Sea $a \equiv 1(mod\ 2)$.

$$|G_a(b)|^2 = \sum_{n_1=0}^{a-1} \sum_{n_2=0}^{a-1} e^{2\pi i \frac{b}{a}(n_1^2 - n_2^2)}.$$

Si hacemos $n_1 = n_2 + m$, entonces para n_2 fijo n_1 recorre con m un sistema completo de restos módulo a, de donde

$$|G_a(b)|^2 = \sum_{m=0}^{a-1} e^{2\pi i \frac{b}{a}m^2} \sum_{n_2=0}^{a-1} e^{4\pi i \frac{b}{a}(mn_2)}.$$

Pero

$$\sum_{n_2=0}^{a-1} e^{4\pi i \frac{b}{a}(mn_2)} = \begin{cases} a & \text{para } m = 0 \\ 0 & \text{para } m \neq 0 \end{cases},$$

de donde

$$|G_a(b)|^2 = a. \tag{5.14}$$

Sea $a \equiv 0(mod\ 4)$. Usando (5.14) y teniendo en cuenta que

$$\sum_{n_2=0}^{a-1} e^{4\pi i \frac{b}{a}(mn_2)} = \begin{cases} a & \text{para } m = 0 \ \wedge \ m = \frac{a}{2} \\ 0 & \text{en otro caso} \end{cases},$$

se tiene

$$|G_a(b)|^2 = \sum_{m=0}^{a-1} e^{2\pi i \frac{b}{a}m^2} \sum_{n_2=0}^{a-1} e^{4\pi i \frac{b}{a}(mn_2)} = 2a.$$

Sea $a \equiv 2(mod\ 4)$. Entonces $a = 2u$ con $u \equiv 1(mod\ 2)$. Aplicando el teorema 5.5.1 y (5.11) se obtiene

$$G_a(b) = G_2(ub)G_u(2b) = 0.$$

Q.e.d.

Los siguientes lemas están dirigidos al cálculo de $G_a(1)$ a través de una representación de las sumas gaussianas cuadráticas como producto.

Lema 5.5.1

Para $n \in \mathbb{N}$ impar y cualquier $x \in \mathbb{R}$ se cumple

$$\prod_{\nu=0}^{n-1} \sin\left(2\pi\left(x + \frac{\nu}{n}\right)\right) = 2^{1-n}(-1)^{\frac{n-1}{2}} \sin(2\pi n x). \tag{5.15}$$

En particular es

$$\prod_{\nu=1}^{\frac{n-1}{2}} \sin\left(2\pi\frac{\nu}{n}\right) = 2^{\frac{1-n}{2}}\sqrt{n} \tag{5.16}$$

$$\prod_{\nu=1}^{\frac{n-1}{2}} \cos\left(2\pi\frac{\nu}{n}\right) = (-1)^{\frac{n^2-1}{8}} 2^{\frac{1-n}{2}}. \tag{5.17}$$

(Los productos vacíos se consideran con el valor 1.)

Demostración: Las soluciones de $z^n - 1 = 0$ (raíces n-ésimas de la unidad) están dadas por $z_\nu = e^{2\pi i\frac{\nu}{n}}$, por lo que

$$\prod_{\nu=0}^{n-1}\left(z - e^{2\pi\frac{\nu}{n}}\right) = z^n - 1.$$

Sea $z = e^{-4\pi ix}$. Entonces

$$\prod_{\nu=0}^{n-1}\left(e^{-4\pi ix} - e^{2\pi\frac{\nu}{n}}\right) = e^{-4\pi inx} - 1.$$

Multiplicando esta igualdad por

$$\prod_{\nu=0}^{n-1}\left(-e^{2\pi(x-\frac{\nu}{n})}\right) = -e^{2\pi inx}$$

se obtiene

$$\prod_{\nu=0}^{n-1}\left(-e^{2\pi(x+\frac{\nu}{n})} - e^{-2\pi(x-\frac{\nu}{n})}\right) = e^{2\pi inx} - e^{2\pi inx},$$

lo que demuestra (5.15).

Ahora

$$\prod_{\nu=1}^{n-1} \sin\left(2\pi\left(x + \frac{\nu}{n}\right)\right) = 2^{1-n}(-1)^{\frac{n-1}{2}}\frac{\sin(2\pi nx)}{\sin(2\pi x)}$$

y pasando al límite cuando $x \to 0$ se obtiene

$$\prod_{\nu=1}^{n-1} \sin\left(2\pi\frac{\nu}{n}\right) = 2^{1-n}(-1)^{\frac{n-1}{2}} n.$$

Entonces

$$\prod_{\nu=1}^{\frac{n-1}{2}} \sin\left(2\pi\frac{\nu}{n}\right)\sin\left(2\pi\frac{n-\nu}{n}\right) = 2^{1-n}(-1)^{\frac{n-1}{2}} n$$

$$\prod_{\nu=1}^{\frac{n-1}{2}} \sin^2\left(2\pi\frac{\nu}{n}\right) = 2^{1-n} n.$$

Pero $\sin\left(2\pi\frac{\nu}{n}\right) > 0$ para $1 \leq \nu \leq \frac{n-1}{2}$, lo que implica (5.16).

Para (5.17) sustituimos en (5.15) a $x = \frac{1}{4}$.

$$\begin{aligned}
\prod_{\nu=1}^{n-1} \cos\left(2\pi\frac{\nu}{n}\right) &= 2^{1-n}, \\
\prod_{\nu=1}^{\frac{n-1}{2}} \cos^2\left(2\pi\frac{\nu}{n}\right) &= 2^{1-n}, \\
\prod_{\nu=1}^{\frac{n-1}{2}} \cos\left(2\pi\frac{\nu}{n}\right) &= \pm 2^{\frac{1-n}{2}}.
\end{aligned}$$

Pero $\cos\left(2\pi\frac{\nu}{n}\right) > 0$ para $1 \leq \nu \leq \frac{n}{4}$ y $\cos\left(2\pi\frac{\nu}{n}\right) < 0$ para $\frac{n}{4} < \nu \leq \frac{n-1}{2}$. Entonces en (5.17) aparece $\frac{n-1}{2} - \left[\frac{n}{4}\right]$ veces el signo menos y por cálculos sencillos se comprueba que

$$\frac{n-1}{2} - \left[\frac{n}{4}\right] \equiv \frac{n^2-1}{8} (mod\ 2),$$

de donde se deduce (5.17). **Q.e.d.**

LEMA 5.5.2

Si $c_0(x,n) = 1$ *y*

$$c_\nu(x,n) = \prod_{k=1}^{\nu} \frac{1-x^{n-k+1}}{1-x^k} \qquad (\nu = 1, 2, \ldots, n),$$

entonces para n *entero con* $n \geq 2$ *y* $n \equiv 0 (mod\ 2)$ *se cumple*

$$\sum_{\nu=0}^{n} (-1)^\nu c_\nu(x,n) = \prod_{k=1}^{\frac{n}{2}} (1-x^{2k-1}). \tag{5.18}$$

Demostración: El caso $n = 0$ es trivial. Sea n entero con $n \geq 2$. Por la definición de c_ν es

$$\begin{aligned}
c_\nu(x,n) &= \frac{1-x^n}{1-x^{n-\mu}} c_\nu(x, n-1) \\
&= c_\nu(x,n-1) + x^{n-\mu} \frac{1-x^n}{1-x^{n-\mu}} c_\nu(x,n-1) \\
&= c_\nu(x,n-1) + x^{n-\mu} c_{\nu-1}(x,n-1).
\end{aligned}$$

Si denotamos por $f(x,n)$ al miembro izquierdo de (5.18) se tiene

$$\begin{aligned} f(x,n) &= 1+(-1)^n+\sum_{\nu=1}^{n-1}(-1)^\nu c_\nu(x,n) \\ &= 1+(-1)^n+\sum_{\nu=1}^{n-1}(-1)^\nu\left(c_\nu(x,n-1)+x^{n-\mu}c_{\nu-1}(x,n-1)\right) \\ &= \sum_{\nu=1}^{n-1}(-1)^{\nu-1}\left(1-x^{n-\mu}\right)c_{\nu-1}(x,n-1) \\ &= \left(1-x^{n-1}\right)\sum_{\nu=1}^{n-1}(-1)^{\nu-1}c_{\nu-1}(x,n-2) \\ &= \left(1-x^{n-1}\right)f(x,n-2). \end{aligned}$$

Pero $f(x,1)=0$ y $f(x,0)=1$, implican que $f(x,n)=0$ para n impar y se cumple la tesis del teorema para n par. **Q.e.d.**

Teorema 5.5.4

Si $(a,b)=1$ y $a\equiv 1(mod\ 2)$, se cumple

$$G_a(b)=2^{\frac{a-1}{2}}\frac{1+i}{2}(1+i^{-a})\prod_{\nu=1}^{\frac{a-1}{2}}\sin^2\left(2\pi\nu\frac{b}{a}\right). \tag{5.19}$$

Demostración: Aplicamos (5.18) con $n=a-1$ y $x=e^{4\pi i\frac{b}{a}}$.

$$c_\nu(x,a-1)=\prod_{k=1}^{\nu}\frac{1-e^{4\pi i\frac{kb}{a}}}{1-e^{-4\pi i\frac{kb}{a}}}=(-1)^\nu e^{2\pi i\nu(\nu+1)\frac{b}{a}}.$$

Entonces para el miembro izquierdo de (5.18) se tiene

$$\begin{aligned} \sum_{\nu=0}^{a-1}(-1)^\nu c_\nu(x,a-1) &= \sum_{\nu=0}^{a-1}e^{2\pi i\nu(\nu+1)\frac{b}{a}} \\ &= e^{-2\pi i(\frac{a-1}{2})^2\frac{b}{a}}\sum_{\nu=0}^{a-1}e^{2\pi i(\frac{a-1}{2}-\nu)^2\frac{b}{a}} \\ &= e^{-2\pi i(\frac{a-1}{2})^2\frac{b}{a}}G_a(b), \end{aligned}$$

es decir

$$\sum_{\nu=0}^{a-1}(-1)^\nu c_\nu(x,a-1)=e^{-2\pi i(\frac{a-1}{2})^2\frac{b}{a}}G_a(b). \tag{5.20}$$

Y para el miembro derecho de (5.18) es

$$\begin{aligned}\prod_{k=1}^{\frac{a-1}{2}}(1-x^{2k-1}) &= \prod_{k=1}^{\frac{a-1}{2}}\left(1-e^{-4\pi i(2k-1)\frac{b}{a}}\right)\\ &= e^{-2\pi i(2k-1)(\frac{a-1}{2})^2\frac{b}{a}}(2i)^{\frac{a-1}{2}}\prod_{k=1}^{\frac{a-1}{2}}\sin\left(2\pi(2k-1)\frac{b}{a}\right).\end{aligned}$$

es decir,

$$\prod_{k=1}^{\frac{a-1}{2}}(1-x^{2k-1}) = e^{-2\pi i(2k-1)(\frac{a-1}{2})^2\frac{b}{a}}(2i)^{\frac{a-1}{2}}\prod_{k=1}^{\frac{a-1}{2}}\sin\left(2\pi(2k-1)\frac{b}{a}\right). \tag{5.21}$$

Primer caso: $a \equiv 1(mod\ 4)$. Los números impares menores que $\frac{a-1}{2}$ son $2k-1$ para $1 \leq k \leq \frac{a-1}{4}$. Para $\frac{a+3}{4} \leq k \leq \frac{a-1}{2}$ es

$$\sin\left(2\pi(2k-1)\frac{b}{a}\right) = \sin\left(2\pi(a-2k')\frac{b}{a}\right) = -\sin\left(2\pi 2k'\frac{b}{a}\right),$$

con $k' = \frac{a+1}{2} - k$. Entonces $2k'$ son los números pares menores que $\frac{a-1}{2}$. A esto se agregan $\frac{a-1}{4}$ signos de menos. Aplicando (5.21) se tiene

$$\prod_{k=1}^{\frac{a-1}{2}}(1-x^{2k-1}) = e^{-2\pi i(\frac{a-1}{2})^2\frac{b}{a}}2^{\frac{a-1}{2}}\prod_{\nu=1}^{\frac{a-1}{2}}\sin\left(2\pi\nu\frac{b}{a}\right). \tag{5.22}$$

Segundo caso: $a \equiv 3(mod\ 4)$. Los números impares menores que $\frac{a-1}{2}$ son $2k-1$ para $1 \leq k \leq \frac{a-1}{4}$. Para $\frac{a+5}{4} \leq k \leq \frac{a-1}{2}$ es

$$\sin\left(2\pi(2k-1)\frac{b}{a}\right) = -\sin\left(2\pi 2k'\frac{b}{a}\right),$$

con $k' = \frac{a+1}{2} - k$. Entonces obtenemos los números pares $2k'$ menores que $\frac{a-1}{2}$ con agregan $\frac{a-3}{4}$ signos de menos. Aplicando (5.21) se tiene

$$\prod_{k=1}^{\frac{a-1}{2}}(1-x^{2k-1}) = e^{-2\pi i(\frac{a-1}{2})^2\frac{b}{a}}i2^{\frac{a-1}{2}}\prod_{\nu=1}^{\frac{a-1}{2}}\sin\left(2\pi\nu\frac{b}{a}\right). \tag{5.23}$$

A partir de (5.18) se obtiene entonces por una parte la identidad de (5.20) y (5.22) y por la otra parte de (5.20) y (5.23). De ambas juntas se deduce (5.19). **Q.e.d.**

TEOREMA 5.5.5 ***Gauss***

$$G_a(1) = \frac{1+i}{2}(1+i)^{-a}\sqrt{a}. \tag{5.24}$$

Demostración:

Para $a \equiv 2(mod\ 4)$ la fórmula (5.24) se deduce de (5.13).

Para $a \equiv 2(mod\ 4)$ la fórmula (5.24) se deduce de (5.16) y (5.19).

Para $a \equiv 1(mod\ 2)$ hacemos $a = 2^\alpha u$ con $\alpha \geq 2$ y $u \equiv 1(mod\ 2)$. Por (5.13) es

$$G_a(1) = G_{2^\alpha}(u) G_u(2^\alpha).$$

Si α es impar, entonces

$$G_u(2^\alpha) = G_u(2),$$

por lo que de (5.19) se tiene

$$G_u(2^\alpha) = 2^{\frac{u-1}{2}} \frac{i+1}{2}(1+i^{-u}) \prod_{\nu=1}^{\frac{u-1}{2}} \sin \frac{4\pi\nu}{u},$$

y aplicando (5.16) y (5.17) es

$$G_u(2^\alpha) = 2^{\frac{u^2-1}{8}} \frac{i+1}{2}(1+i^{-u})\sqrt{u}.$$

Finalmente, por (5.12) es

$$G_u(1) = 2^{\frac{u^2-1}{8}} \frac{i+1}{\sqrt{2}}(1+i^{-u}) e^{\pi i \frac{u}{4}} \sqrt{a} = (1+i)\sqrt{a}.$$

Q.e.d.

TEOREMA 5.5.6 ***Gauss***

Si $a, b \in \mathbb{N}$ con $(a,b) = 1$ y $b \equiv 1(mod\ 2)$, entonces

$$G_a(b) = \sqrt{\frac{a}{b}} \frac{1+i}{2}(1+i)^{-ab} \overline{G_b(a)}. \tag{5.25}$$

Demostración: Del teorema 5.5.1, para $(a,b) = 1$ se cumple

$$G_a(b) G_b(a) = G_{ab}(1),$$

y multiplicando por $\overline{G_b(a)}$ es

$$G_a(b) |G_b(a)|^2 = G_{ab}(1) \overline{G_b(a)}.$$

Por (5.13) es

$$|G_b(a)|^2 = b \qquad \text{para} \qquad b \equiv 1(mod\ 2).$$

Aplicando (5.24) se tiene

$$G_{ab}(1) = \frac{1+i}{2}(1+i)^{-ab}\sqrt{ab}.$$

De lo anterior se deduce el teorema. **Q.e.d.**

APLICACIÓN A LOS RESIDUOS CUADRÁTICOS

Sea p primo impar y q un número entero cualquiera con $(p,q)=1$. Por el teorema 5.4.2 (5.10) y por la definición 5.5.1 es

$$G_p(q) = \left(\frac{q}{p}\right) G_p(1).$$

Al aplicar (5.19) se tiene

$$\left(\frac{q}{p}\right) = \prod_{\nu=1}^{\frac{p-1}{2}} \frac{\sin\left(2\pi\nu\frac{q}{p}\right)}{\sin\left(2\pi\nu\frac{1}{p}\right)}, \tag{5.26}$$

o con (5.16)

$$\left(\frac{q}{p}\right) = \frac{2^{\frac{p-1}{2}}}{\sqrt{p}} \prod_{\nu=1}^{\frac{p-1}{2}} \sin\left(2\pi\nu\frac{q}{p}\right). \tag{5.27}$$

Sin dificultad se pueden deducir ahora de (5.27), usando (5.16) y (5.17), los teoremas complementarios de la ley de reciprocidad cuadrática

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

DOS NUEVAS VARIANTES DE DEMOSTRACIÓN DE LA LEY DE RECIPROCIDAD CUADRÁTICA

Sean p, q primos impares con $p \neq q$.

VARIANTE 1: Utilización de la representación en producto (5.26) del símbolo de Legendre.

(Atención: (5.26) sólo se puede deducir del criterio de Euler y del lema 5.5.1). Por (5.15) es

$$\begin{aligned}\frac{\sin\left(2\pi\nu\frac{q}{p}\right)}{\sin\left(2\pi\nu\frac{1}{p}\right)} &= 2^{q-1}(-1)^{\frac{q-1}{2}} \prod_{\nu'=1}^{q-1} \sin\left(2\pi\left(\frac{\nu}{p}+\frac{\nu'}{p}\right)\right) \\ &= (-4)^{\frac{q-1}{2}} \prod_{\nu'=1}^{\frac{q-1}{2}} \sin\left(2\pi\left(\frac{\nu}{p}+\frac{\nu'}{p}\right)\right)\sin\left(2\pi\left(\frac{\nu}{p}-\frac{\nu'}{p}\right)\right).\end{aligned}$$

Sustituyendo en (5.26) es

$$\left(\frac{q}{p}\right) = (-4)^{\frac{(p-1)(q-1)}{2}} \prod_{\nu=1}^{\frac{p-1}{2}} \prod_{\nu'=1}^{\frac{q-1}{2}} \sin\left(2\pi\left(\frac{\nu}{p}+\frac{\nu'}{p}\right)\right) \sin\left(2\pi\left(\frac{\nu}{p}-\frac{\nu'}{p}\right)\right),$$

e intercambiando p y q se obtiene

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

Q.e.d.

VARIANTE 2: Utilización de la ley de reciprocidad (5.25) de las sumas gaussianas.

Se cumple

$$G_p(q) = \left(\frac{q}{p}\right) G_q(p).$$

Aplicando (5.24), como p es impar, se tiene

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

y por (5.25) es

$$G_p(q) = \sqrt{\frac{p}{q}} i^{\left(\frac{pq-1}{2}\right)^2} \overline{G_q(p)}.$$

Sustituyendo se obtiene

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

Q.e.d.

5.6. Ejercicios del capítulo

1. Determine el producto de todos los elementos de un grupo abeliano finito.
2. Determine todos los grupos abelianos de orden 6, 18 y 30 y sus particiones en productos directos de grupos cíclicos.
3. Determine todos los grupos abelianos de orden 8 y los correspondientes caracteres de cada grupo.

4. Sea p un número primo, que no divide a b y sea $\nu \geq 2$. Demuestre que

$$G_{p^\nu}(b) = pG_{p^{\nu-2}}(b),$$

y deduzca de ello que

$$G_{p^\nu} = \begin{cases} p^{\frac{\nu}{2}} & \nu \equiv 0(mod\ 2) \\ p^{\frac{\nu-1}{2}} G_p(b) & \nu \equiv 1(mod\ 2) \end{cases}.$$

5. Sea p un número primo, que no divide a b y sea $\nu \equiv 1(mod\ 2)$. Demuestre que

$$G_{p^\nu}(b) = \begin{cases} \left(\frac{b}{p}\right) p^{\frac{\nu}{2}} & p \equiv 1(mod\ 4) \\ i\left(\frac{b}{p}\right) p^{\frac{\nu}{2}} G_p(b) & p \equiv 3(mod\ 4) \end{cases}.$$

Capítulo 6

NÚMEROS ALGEBRAICOS Y TRASCENDENTES

6.1. Fracciones continuas

Se conoce que todo número real puede ser expresado en notación decimal. Así, por ejemplo, si $0 \leq r \leq 1$, entonces es

$$r = \sum_{n=1}^{\infty} a_n 10^{-n} = 0.a_2a_2a_3 \ldots .$$

Además se conoce que r es racional si ese desarrollo es periódico (es decir si existe un entero m, tal que $a_{k+m} = a_k$ para todo índice k). Pero resulta complicado determinar por esta vía si un número es racional o no, pues el período puede ser excesivamente grande. Esto da pie al desarrollo en fracciones continuas.

Si $a_0, a_1 \in \mathbb{N}$ con $a_0 > a_1 > 1$, aplicando el algoritmo de Euclides se tiene

$$\begin{array}{rcll} \dfrac{a_0}{a_1} & = & q_1 + \dfrac{a_2}{a_1} & \text{con} \quad 0 < \dfrac{a_2}{a_1} < 1, \\ \dfrac{a_1}{a_2} & = & q_2 + \dfrac{a_3}{a_2} & \text{con} \quad 0 < \dfrac{a_3}{a_2} < 1, \\ \cdots & \cdots & \cdots & \\ \dfrac{a_{n-2}}{a_{n-1}} & = & q_{n-1} + \dfrac{a_n}{a_{n-1}} & \text{con} \quad 0 < \dfrac{a_n}{a_{n-1}} < 1, \\ \dfrac{a_{n-1}}{a_n} & = & q_n. & \end{array}$$

Al sustituir todas las ecuaciones en la primera se obtiene

$$\frac{a_0}{a_1} = q_1 + \frac{1}{q_2 + \frac{a_3}{a_2}} = \ldots = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \frac{1}{q_n}}}}}.$$

Ello da lugar a la siguiente definición (que será considerada formalmente hasta tanto no se demuestre convergencia).

DEFINICIÓN 6.1.1

Una ***fracción continua*** *es el desarrollo*

$$[a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \ldots}}.$$

donde $a_0 \in \mathbb{R}$ *y los* $a_1, a_2, \ldots$ *son números positivos.*

Los números $a_0, a_1, a_2, \ldots$ *se llaman* ***cocientes parciales*** *y la fracción continua se dice* ***simple*** *si* a_k *es entero para todo* k*.*

Si la sucesión $\{a_n\}$ *es infinita se habla de* ***fracción continua infinita****.*

La parte finita $[a_0; a_1, a_2, \ldots, a_k]$ *se llama* ***corte*** k***-ésimo*** *de la fracción continua* $[a_0; a_1, a_2, \ldots]$*.*

Muchos historiadores de la Matemática conciden en considerar que la teoría de las fracciones continuas comenzó con Rafael Bombelli[1], el último de los grandes algebristas del Renacentismo italiano. En su "L' Algebra Opera" (1572), Bombelli intenta encontrar raíces cuadradas como núcleos de fracciones continuas infinitas, un método ingenioso y novedoso. El demostró que $\sqrt{13}$ se puede expresar como la fracción continua

$$\sqrt{13} = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 + \ddots}}}.$$

Bombelli fue el primero en popularizar la "Arithmetica" de Diofanto en el occidente latino, que comenzó a traducir de la copia de la Biblioteca del Vaticano. Aunque no pudo terminar la traducción, incluyó en su libro todos los problemas de los primeros cuatro libros.

EJEMPLO: Veamos el caso particular del número racional $\frac{62}{23}$.

Por el algoritmo de Euclides es

$$\begin{aligned} 62 &= 2(23) + 16 \\ 23 &= 1(16) + 7 \\ 16 &= 2(7) + 2 \\ 7 &= 3(2) + 1. \end{aligned}$$

[1]Rafael Bombelli (1530-1573)

Entonces

$$\begin{aligned}\frac{62}{23} &= 2+\frac{16}{23} = 2+\frac{1}{\frac{23}{16}}\\ \frac{23}{16} &= 1+\frac{7}{16} = 1+\frac{1}{\frac{16}{7}}\\ \frac{16}{7} &= 2+\frac{2}{7} = 2+\frac{1}{\frac{7}{2}}\\ \frac{7}{2} &= 3+\frac{1}{2}.\end{aligned}$$

Entonces es

$$\frac{62}{23} = 2+\frac{1}{1+\frac{1}{2+\frac{1}{3+\frac{1}{2}}}} = [2;1,2,3,2].$$

Nótese que para este número racional se ha obtenido una fracción continua finita. Es más, siguiendo este ejemplo, se puede observar que el algoritmo de la división de Euclides parece garantizar que todo número racional $\frac{p}{q}$ tiene un desarrollo en fracciones continuas finito. ¿Será válido el recíproco?

TEOREMA 6.1.1

Toda fracción continua simple es finita si y solo si representa un número racional.

Demostración: (Necesidad: por inducción)

(i) Para $n=1$ es $[a_0;a_1] = a_0+\frac{1}{a_1}$, que representa un número racional.

(ii) Supongamos que toda fracción continua simple finita $[b_0;b_1,b_2,\ldots,b_n]$ de $n+1$ cocientes parciales representa un número racional $\frac{p}{q}$.

(iii) Para la fracción continua simple de $n+2$ cocientes parciales se tiene

$$[a_0;a_1,\ldots,a_n,a_{n+1}] = a_0+\frac{1}{[a_1;a_2,a_3,\ldots,a_n]} = a_0+\frac{q}{p},$$

que es un número racional.

(Suficiencia) Sea $x=\frac{a}{b}$ con a,b y $b>0$. Sea $r_0=a$ y $r_1=b$. Aplicando el algoritmo de la división de Euclides se tiene

$$\begin{aligned}r_0 &= r_1q_1+r_2 \quad \text{con} \quad 0\le r_2<r_1\\ r_1 &= r_1q_2+r_3 \quad \text{con} \quad 0\le r_3<r_2\\ \ldots &\quad \ldots \quad \ldots\\ r_{n-3} &= r_{n-2}q_{n-2}+r_{n-1} \quad \text{con} \quad 0\le r_{n-1}<r_{n-2}\\ r_{n-2} &= r_{n-1}q_{n-1}+r_n \quad \text{con} \quad 0\le r_n<r_{n-1}\\ r_{n-1} &= r_nq_n.\end{aligned}$$

Desarrollando entonces de modo análogo al ejemplo se obtiene

$$\frac{a}{b} = [q_1; q_2, q_3, \ldots, q_n].$$

Q.e.d.

De todo lo anterior se deduce que el desarrollo en fracciones continuas es mejor que el desarrollo en fracciones decimales para determinar si un número es racional o no.

Sin embargo, la representación de un número en fracciones continuas simples no es único, pues como $a_n = (a_n - 1) + \frac{1}{1}$, entonces

$$[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_{n-1}, a_n - 1, 1].$$

Así se tiene que

Todo número racional tiene exactamente dos representaciones en fracciones continuas simples, una con un número par y otra con un número impar de términos.

Veamos con mas detalle las fracciones continuas infinitas y sus cortes k-ésimos.

TEOREMA 6.1.2

Sean p_k, q_k definidos como

$$\begin{aligned} p_{-1} &= 1, \quad p_0 = a_0, \quad p_k = a_k p_{k-1} + p_{k-2} \qquad (k \geq 1) \\ q_{-1} &= 0, \quad q_0 = 1, \quad q_k = a_k q_{k-1} + q_{k-2} \qquad (k \geq 1). \end{aligned}$$

Entonces todo corte k-ésimo de la fracción continua $[a_0; a_1, a_2, \ldots]$ se puede representar en la forma

$$[a_0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k} \qquad (k \geq 0).$$

La fracción $C_k = \frac{p_k}{q_k}$ se conoce como aproximación racional de orden k *de* $[a_0; a_1, a_2, \ldots]$.

Demostración: (Inducción)

(i) Para $k = 0$ es obvio, pues

$$[a_0] = a_0 = \frac{p_0}{q_0}.$$

Para $k = 1$ es

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{a_1 p_0 + p_{-1}}{q_1} = \frac{p_1}{q_1}.$$

(ii) Sea válido el teorema para $k \leq n$.

(iii) Para $k = n+1$ es

$$\begin{aligned}[a_0; a_1, \ldots, a_{n+1}] &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}}} \\ &= \left[a_0; a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right]\end{aligned}$$

Pero por (ii) es

$$\left[a_0; a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right] = \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}},$$

de donde

$$\begin{aligned}[a_0; a_1, \ldots, a_{n+1}] &= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \\ &= \frac{(a_{n+1}a_n + 1)p_{n-1} + a_{n+1}p_{n-2}}{(a_{n+1}a_n + 1)q_{n-1} + a_{n+1}q_{n-2}} \\ &= \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}.\end{aligned}$$

Q.e.d.

TEOREMA 6.1.3

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}, \quad \textit{para } k \geq 0 \tag{6.1}$$
$$q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k \quad \textit{para } k \geq 1. \tag{6.2}$$

Demostración: Por el teorema 6.1.2 es

$$p_k = a_k p_{k-1} + p_{k-2} \tag{6.3}$$
$$q_k = a_k q_{k-1} + q_{k-2}. \tag{6.4}$$

Multiplicando (6.3) por q_{k-1} y (6.4) por p_{k-1} y restando, se obtiene

$$\begin{aligned}p_k q_{k-1} - p_{k-1} q_k &= a_k p_{k-1} q_{k-1} + p_{k-2} q_{k-1} - a_k p_{k-1} q_{k-1} - p_{k-1} q_{k-2} \\ &= p_{k-2} q_{k-1} - p_{k-1} q_{k-2} \\ &= -\left(p_{k-1} q_{k-2} - p_{k-2} q_{k-1}\right) = \ldots \\ &= (-1)^k \left(p_0 q_{-1} - p_{-1} q_0\right) = (-1)^{k-1}.\end{aligned}$$

Multiplicando ahora (6.4) por p_{k-2} y (6.3) por q_{k-2} y restando, se obtiene

$$\begin{aligned} q_k p_{k-2} - p_k q_{k-2} &= a_k q_{k-1} p_{k-2} + p_{k-2} q_{k-2} - a_k p_{k-1} q_{k-2} - p_{k-2} q_{k-2} \\ &= a_k \left(q_{k-1} p_{k-2} - p_{k-1} q_{k-2} \right) \\ &= a_k (-1) \left(p_{k-1} q_{k-2} - p_{k-2} q_{k-1} \right) = \dots \\ &= a_k (-1)^{k+1} = (-1)^{k-1} a_k. \end{aligned}$$

Q.e.d.

NOTA: De (6.2) se deduce

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}} \qquad (k \geq 2).$$

De (6.1) se deduce que $(p_k, q_k) = 1$ y

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1} a_k}{q_k q_{k-1}}.$$

Esto se resume en el siguiente corolario:

Corolario 6.1.1

Sea $C_k = \frac{p_k}{q_k}$ la k-ésima aproximación de $[a_0; a_1, a_2, \dots]$ para $1 \leq k \leq n$. Entonces $(p_k, q_k) = 1$ y se cumple

$$C_1 > C_3 > C_5 > \dots,$$
$$C_0 < C_2 < C_4 < \dots,$$
$$C_{2j+1} > C_{2j} \quad \text{para todo } j.$$

En otras palabras

- *Las aproximaciones racionales de orden par forman una sucesión estrictamente monótona creciente.*
- *Las aproximaciones racionales de orden impar forman una sucesión estrictamente monótona decreciente.*
- *Toda aproximación racional de orden impar es mayor que toda aproximación racional de orden par.*

Luego, si el número $\alpha \in \mathbb{R}$ se puede representar por la fracción continua finita $[a_0; a_1, \dots, a_n]$, entonces para $2k + 1 < n$ es

$$\frac{p_{2k}}{q_{2k}} < \alpha < \frac{p_{2k+1}}{q_{2k+1}} \qquad \text{y} \qquad \alpha = \frac{p_n}{q_n}. \tag{6.5}$$

Por otra parte, toda fracción continua infinita se corresponde a una sucesión $\left\{\frac{p_n}{q_n}\right\}$ de aproximaciones racionales. En ese caso es

$$\alpha = [a_0; a_1, a_2, \ldots] \qquad \text{para} \qquad \lim_n \frac{p_n}{q_n} = \alpha \text{ (si existe).}$$

Para la sucesión de aproximaciones racionales $\left\{\frac{p_n}{q_n}\right\}$ se cumple siempre la desigualdad (6.5).

EJEMPLO: Para la fracción continua $[2; 3, 1, 1, 2, 4]$ se tiene

$$C_0 = 2, \qquad C_1 = \tfrac{7}{3} = 2{,}33\ldots, \qquad C_2 = \tfrac{9}{4} = 2{,}25\ldots,$$

$$C_3 = \tfrac{16}{7} = 2{,}2857, \quad C_4 = \tfrac{41}{18} = 2{,}2777, \quad C_5 = \tfrac{180}{79} = 2{,}2784\ldots,$$

y se cumple

$$2 < 2,25 < 2,2777, \ldots$$

$$2{,}33 > 2{,}2857 > 2{,}2784 > \ldots.$$

Las fracciones continuas finitas se aplican también a la ecuación diofántica lineal

$$ax + by = c,$$

donde a, b, c son enteros dados. Asumamos que $d|c$ para $d = (a, b)$, pues en caso contrario no existe solución de la ecuación. Más aún, podemos asumir sin perder generalidad que a y b son primos relativos, pues en otro caso, dividiendo la ecuación por d se obtiene una ecuación equivalente a la original, con las mismas soluciones.

Recordemos también que si $(a, b) = 1$, de la solución (x_0, y_0) de la ecuación diofántica

$$ax + by = 1$$

Se obtiene, multiplicando por c, la solución (cx_0, cy_0) de la ecuación

$$ax + by = c.$$

Para encontrar la solución de la ecuación $ax + by = 1$ se desarrolla en fracciones continuas el número racional $\frac{a}{b}$. Sea

$$\frac{a}{b} = [a_0; a_1, \ldots . a_n].$$

Las últimas k-ésimas aproximaciones de esta fración continua son

$$C_{n-1} = \frac{p_{n-1}}{q_{n-1}}, \qquad C_n = \frac{p_n}{q_n} = \frac{a}{b}.$$

Como $(p_n, q_n) = (a, b) = 1$, se concluye que

$$p_n = a \qquad q_n = b.$$

Al aplicar el teorema 6.1.3 se obtiene

$$aq_{n-1} - bp_{n-1} = (-1)^{n-1}.$$

Haciendo $x = q_{n-1}$, $y = p_{n-1}$ se obtiene

$$ax - by = (-1)^{n-1}.$$

Si n es impar, la ecuación $ax + by = 1$ tiene la solución particular $x_0 = q_{n-1}$, $y_0 = -p_{n-1}$, mientras que, si n es par, la solución está dada por $x_0 = -q_{n-1}$, $y_0 = p_{n-1}$. Entonces la solución general es (como ya se ha visto)

$$x = x_0 + bt, \quad y = y_0 - at, \qquad (t = 0, \pm 1, \pm 2, \ldots).$$

EJEMPLO: Considere la ecuación diofántica

$$172x + 20y = 100.$$

Como $(172, 20) = 4$, esta ecuación se sustituye por la ecuación

$$43x + 5y = 250.$$

El primer paso es encontrar una solución particular de

$$43x + 5y = 1.$$

Para ello ello se escribe $\frac{43}{5}$ (o su recíproco) como fracción continua. La aplicación del algoritmo de Euclides produce

$$\begin{aligned} 43 &= 8 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1, \\ 2 &= 2 \cdot 1, \end{aligned}$$

de modo que

$$\frac{43}{5} = [8; 1, 1, 2] = 8 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}.$$

Las k-ésimas aproximaciones de la fracción continua son

$$C_0 = \frac{8}{1}, \quad C_1 = \frac{9}{1}, \quad C_2 = \frac{17}{2}, \quad C_3 = \frac{43}{5},$$

de donde se deduce que $p_2 = 17$, $q_2 = 2$, $p_3 = 43$ y $q_3 = 5$. Por el teorema 6.3 es

$$p_3q_2 - q_3p_2 = (-1)^{3-1};$$

es decir

$$43 \cdot 2 - 5 \cdot 17 = 1.$$

Al multiplicar por 250 es

$$43(500) - 5(-4250) = 250.$$

Entonces una solución particular de la ecuación diofántica lineal $43x + 5y = 250$ es

$$x_0 = 500, \qquad y_0 = -4250,$$

y la solución general es

$$x = 500x_0 + 5t, \quad y = -4250 - 43t, \qquad (t = 0, \pm 1, \pm 2, \ldots).$$

Pero... ¿Qué sucede con las fracciones continuas infinitas? ¿Cuándo tienen sentido? Para responder a estas preguntas se necesitan los resultados del Análisis Matemático referentes a la convergencia de sucesiones monótonas crecientes (decrecientes) y acotadas superiormente (inferiormente).

A partir de ahora se considera $a_0 \in \mathbb{Z}$, $a_1, a_2, \ldots \in \mathbb{N}$ y el último $a_n \neq 1$ para fracciones continuas simples finitas.

TEOREMA 6.1.4 *Toda fracción continua simple es convergente.*

Demostración: Basta demostrar que $\left\{\frac{p_n}{q_n}\right\}$ cumple el criterio de convergencia de Cauchy, es decir,

$$\forall \varepsilon > 0 \quad \exists n_0 \in \mathbb{N}; \quad \left|\frac{p_k}{q_k} - \frac{p_m}{q_m}\right| < \varepsilon \quad \forall k, m \geq n_0.$$

Sea (sin perder generalidad) $k > m$, entonces por el teorema 6.1.3 es

$$\left|\frac{p_k}{q_k} - \frac{p_m}{q_m}\right| \leq \sum_{i=m}^{k-1} \left|\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i}\right| = \sum_{i=m}^{k-1} \frac{1}{q_i q_{i+1}}.$$

Pero $a_1, a_2, \ldots \in \mathbb{N}$ (son positivos), por lo que $q_1 = a_1 \geq 1$ (vea teorema 6.1.2), y $q_k \geq q_{k-1} + 1$ para $k \geq 2$, de donde $q_k \geq k$. Entonces

$$\left|\frac{p_k}{q_k} - \frac{p_m}{q_m}\right| \leq \sum_{i=m}^{k-1} \frac{1}{i(i+1)} = \sum_{i=m}^{k-1} \left(\frac{1}{i} - \frac{1}{i+1}\right) = \frac{1}{m} - \frac{1}{k} < \frac{1}{m}.$$

Luego, si $\frac{1}{n_0} < \varepsilon$, se cumple

$$\left|\frac{p_k}{q_k} - \frac{p_m}{q_m}\right| < \frac{1}{m} \leq \frac{1}{n_0} < \varepsilon.$$

Q.e.d.

A partir de lo ya conocido se obtiene el siguiente resultado general.

Teorema 6.1.5

Todo $\alpha \in \mathbb{R}$ se puede expresar de modo único en una fracción continua simple. La correspondiente fracción continua es finita si α es racional y es infinita si α es irracional.

Demostración: La existencia de la representación ya ha sido demostrada anteriormente, así como la clasificación de las fracciones continuas simples en finitas o infitas según sea α racional o irracional.

Veamos que para α irracional

$$\lim_n \frac{p_n}{q_n} = \alpha.$$

Desarrollando es

$$\alpha - \frac{p_n}{q_n} = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(r_{n+1}q_n + q_{n-1})}.$$

Por la identidad (6.1) del teorema 6.1.3 es

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(r_{n+1}q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_nq_{n+1}}. \tag{6.6}$$

Pero $q_n \to \infty$, por lo que

$$\lim_n \frac{p_n}{q_n} = \alpha.$$

Resta demostrar la unicidad. Supongamos que

$$\alpha = [a_0; a_1, a_2, \ldots] = [a'_0; a'_1, a'_2, \ldots].$$

Obviamente es

$$[\alpha] = a_0 = a'_0.$$

Supongamos que $a_k = a'_k$ para $k \leq n$. Entonces para $k \leq n$ es

$$p_k = p'_k, \qquad q_k = q'_k.$$

Luego,

$$\alpha = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}} = \frac{r'_{n+1}p'_n + p'_{n-1}}{r'_{n+1}q'_n + q'_{n-1}} = \frac{r'_{n+1}p_n + p_{n-1}}{r'_{n+1}q_n + q_{n-1}},$$

por lo que $r_{n+1} = r'_{n+1}$ y como

$$a_{n+1} = [r_{n+1}], \qquad a'_{n+1} = [r'_{n+1}],$$

entonces $a_{n+1} = a'_{n+1}$. **Q.e.d.**

VENTAJAS DEL DESARROLLO EN FRACCIONES CONTINUAS

- Se logra una separación exacta entre números racionales e irracionales
- Cuando se corta el desarrollo en un paso determinado, entonces cualquier nuevo desarrollo produce una aproximación racional mejor (ello se observa en (6.6)).

Teorema 6.1.6

Si $\frac{p_n}{q_n}$ es la n-ésima aproximación racional del desarrollo en fracciones continuas de $\alpha \in \mathbb{R}$, entonces se cumple

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

Demostración: Se demostró en el teorema anterior. **Q.e.d.**

Definición 6.1.2

Toda solución no racional de la ecuación

$$ax^2 + bx + c = 0 \qquad con \qquad a, b, c \in \mathbb{Z}, \quad a \neq 0$$

se llama ***irracionalidad cuadrática****.*

La fracción continua infinita $\alpha = [a_0; a_1, a_2, \ldots]$ se dice ***periódica****, si existen $n \geq 0$ y $h \geq 1$ enteros con $a_{k+h} = a_k$ para todo $k \geq n$. En ese caso se escribe*

$$\alpha = [a_0; a_1, a_2, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+h}}].$$

Teorema 6.1.7

Toda fracción continua periódica representa una irracionalidad cuadrática. Recíprocamente, toda irracionalidad cuadrática tiene un desarrollo en fracción continua periódica.

Demostración:

(Necesidad) Sea

$$\alpha = [a_0; a_1, a_2, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+h}}]$$

y sea

$$r_n = [a_n; a_{n+1}, \ldots, a_{n+h-1}, a_n, a_{n+1}, \ldots, a_{n+h-1}, \ldots] = [a_n; a_{n+1}, \ldots, a_{n+h-1}, r_n].$$

Si $h = 1$, entonces

$$r_n = [a_n; r_n] = a_n + \frac{1}{r_n},$$

de donde

$$r_n^2 - a_n r_n - 1 = 0.$$

Si $h \neq 1$, sean $\frac{p''}{q''}$ y $\frac{p'}{q'}$ las dos últimas aproximaciones racionales de $[a_n; a_{n+1}, \ldots, a_{n+h-1}]$, donde excepcionalmente puede ser $a_{n+h-1} = 1$. Por el teorema 6.1.2 es

$$r_n = \frac{r_n p' + p''}{r_n q' + q''},$$

por lo que r_n satisface una ecuación cuadrática $ax^2 + bx + c = 0$ con $a, b, c \in \mathbb{Z}$ y $a \neq 0$, pues $q' \neq 0$.

Ahora es

$$\alpha = [a_0; a_1, a_2, \ldots, a_{n-1}, r_n] = \frac{r_n p_{n-1} + p_{n-2}}{r_n q_{n-1} + q_{n-2}}, \qquad (n \geq 1).$$

Entonces

$$r_n(\alpha q_{n-1} - p_{n-1}) - (\alpha q_{n-2} - p_{n-2}) = 0,$$

de donde

$$r_n = \frac{\alpha q_{n-2} - p_{n-2}}{\alpha q_{n-1} - p_{n-1}}.$$

Sustituyendo en $ar_n^2 + br_n + c = 0$ es

$$\frac{a(\alpha^2 q_{n-2}^2 - p_{n-2}^2 - 2\alpha q_{n-2} p_{n-2})}{(\alpha q_{n-1} - p_{n-1})^2} + \frac{b(\alpha q_{n-2} - p_{n-2})}{\alpha q_{n-1} - p_{n-1}} + c = 0,$$

por lo que α satisface una ecuación cuadrática $Ar_n^2 + Br_n + C = 0$ con $A, B, C \in \mathbb{Z}$. Entonces α es una irracionalidad cuadrática.

(Suficiencia) Sea α tal que $A\alpha^2 + B\alpha + C = 0$ con $A, B, C \in \mathbb{Z}$ y $A \neq 0$. Hacemos el desarrollo

$$\alpha = [a_0; a_1, a_2, \ldots] = [a_0; a_1, a_2, \ldots, a_{n-1}, r_n] = \frac{r_n p_{n-1} + p_{n-2}}{r_n q_{n-1} + q_{n-2}}, \qquad (n \geq 1).$$

Entonces es

$$\frac{A(r_n p_{n-1} + p_{n-2})^2}{(r_n q_{n-1} + q_{n-2})^2} + \frac{B(r_n p_{n-1} + p_{n-2})}{r_n q_{n-1} + q_{n-2}} + C = 0,$$

por lo que

$$\begin{aligned} A(r_n^2 p_{n-1}^2 &+ 2r_n p_{n-1} p_{n-2} + p_{n-2}^2) \\ &+ B(r_n^2 p_{n-1} q_{n-1} + r_n(q_{n-2} p_{n-1} + p_{n-2} q_{n-1}) + p_{n-2} q_{n-2}) \\ &+ C(r_n q_{n-1} + q_{n-2})^2 = 0. \end{aligned}$$

De aquí que se cumple

$$A_n r_n^2 + B_n r_n + C_n = 0,$$

con

$$\begin{aligned} A_n &= A p_{n-1}^2 + B p_{n-1} q_{n-1} + C q_{n-1}^2 \neq 0 \\ B_n &= 2A p_{n-1} p_{n-2} + B(p_{n-1} q_{n-2} + p_{n-2} q_{n-1}) + 2C q_{n-1} q_{n-2} \\ C_n &= A p_{n-2}^2 + B p_{n-2} q_{n-2} + C q_{n-1}^2 = A_{n-1}. \end{aligned}$$

Aquí es $A_n \neq =$, pues sino $A\alpha^2 + B\alpha + C = 0$ tendría solución racional. Por el teorema 6.1.6, existe δ_{n-1} tal que

$$p_{n-1} = \alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}} \qquad \text{y} \qquad |\delta_{n-1}| < 1.$$

Entonces

$$\begin{aligned} A_n &= A\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right)^2 + B\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right) q_{n-1} + C q_{n-1}^2 \\ &= A\left(\alpha^2 q_{n-1}^2 + 2\alpha\delta_{n-1} + \frac{\delta_{n-1}^2}{q_{n-1}^2}\right) + B(\alpha q_{n-1}^2 + \delta_{n-1}) + C q_{n-1}^2 \\ &= (A\alpha^2 + B\alpha + C) q_{n-1}^2 + 2A\alpha\delta_{n-1} + B\delta_{n-1} + A\frac{\delta_{n-1}^2}{q_{n-1}^2}. \end{aligned}$$

Pero $A\alpha^2 + B\alpha + C = 0$ y $|\delta_{n-1}| < 1$, por lo que

$$\begin{aligned} |A_n| &\leq 2|A\alpha| + |B| + |A| \\ |C_n| &= |A_{n-1}| < 2|A\alpha| + |A| + |B|. \end{aligned}$$

Además

$$B_n^2 - 4A_n C_n = (B^2 - 4AC)(p_{n-1} q_{n-2} - q_{n-1} p_{n-2})^2 = B^2 - 4AC$$

implica que

$$B_n^2 \leq 4|A_n C_n| + |B^2 - 4AC| < (2|A\alpha| + |B| + |A|)^2 + (B^2 - 4AC).$$

De ello se deduce que A_n, B_n, C_n toman una cantidad finita de valores, por lo que r_n también toma una cantidad finita de valores.

Sea $r_n = r_{n+h}$ para n y h apropiados, de modo que

$$r_n = [a_n; a_{n+1}, \ldots], \qquad r_{n+h} = [a_{n+h}; a_{n+h+1}, \ldots].$$

Entonces es $a_k = a_{k+h}$ para $k \geq n$, por lo que la fracción continua queda unívocamente determinada. **Q.e.d.**

6.2. Aproximación de números reales por racionales

TEOREMA 6.2.1

Para cualesquiera números reales α y η con $\eta \geq 1$ existen enteros p, q que satisfacen

$$|q\alpha - p| < \frac{1}{\eta}, \qquad (1 \leq q \leq \eta).$$

Demostración: Si $\alpha = \frac{a}{b}$ es racional con $1 \leq b \leq \eta$ la afirmación es trivial.

Sea entonces $b > \eta$ o α irracional. Consideremos las aproximaciones racionales $\frac{p_k}{q_k}$ del desarrollo en fracciones continuas de α y determinamos para η un n tal que $q_n \leq \eta < q_{n+1}$. Por (6.6) es

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n \eta},$$

de donde se deduce el teorema. **Q.e.d.**

TEOREMA 6.2.2

Si $\frac{p_n}{q_n}$ es una aproximación racional de α, entonces para todos los números racionales $\frac{p}{q}$ con $0 < q \leq q_n$ tal que $\frac{p}{q} \neq \frac{p_n}{q_n}$, se cumple

$$|q_n\alpha - p_n| < |q\alpha - p|.$$

NOTA: De aquí se deduce que $\frac{p_n}{q_n}$ es la mejor aproximación de α, pues

$$q_n \left|\alpha - \frac{p_n}{q_n}\right| < q \left|\alpha - \frac{p_n}{q_n}\right| < q_n \left|\alpha - \frac{p}{q}\right|.$$

Demostración del teorema: Sea $\alpha \neq \frac{p_n}{q_n}$ (otro caso es trivial). Consideremos la ecuación

$$q\alpha - p = M(q_n\alpha - p_n) + N(q_{n-1}\alpha - p_{n-1}), \tag{6.7}$$

con M, N del sistema de ecuaciones

$$\begin{aligned} Mp_n - Np_{n-1} &= p \\ Mq_n - Nq_{n-1} &= q. \end{aligned}$$

El determinante es

$$\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1},$$

por lo que el sistema tiene solución única

$$N = \frac{\begin{vmatrix} p_n & p \\ q_n & q \end{vmatrix}}{(-1)^{n-1}} = (-1)^{n-1}(p_n q - p q_n) \qquad \Rightarrow \qquad N \in \mathbb{Z}$$

$$M = \frac{\begin{vmatrix} p & p_{n-1} \\ q & q_{n-1} \end{vmatrix}}{(-1)^{n-1}} = (-1)^{n-1}(p q_{n-1} - q p_{n-1}) \qquad \Rightarrow \qquad M \in \mathbb{Z}.$$

Pero $N \neq 0$, pues $\frac{p}{q} \neq \frac{p_n}{q_n}$. Entonces $M = 0$ ó M y N tienen diferentes signos, pues en caso contrario se obtendría una contradicción con $q > q_n$.

Luego, los sumandos en el miembro derecho de (6.7) tienen igual signo, pues también $(q_n\alpha - p_n)$ y $(q_{n-1}\alpha - p_{n-1})$ tiene signos diferentes por tratarse de aproximaciones racionales vecinas. De aquí que

$$|q\alpha - p| = |M(q_n\alpha - p_n)| + |N(q_{n-1}\alpha - p_{n-1})| \geq |q_{n-1}\alpha - p_{n-1}|.$$

En $\alpha = [a_0; a_1, \ldots, a_n, r_{n+1}]$ es $r_{n+1} > 1$ (sólo se consideran tales fracciones continuas) y

$$\alpha = \frac{p_n r_{n+1} + p_{n-1}}{q_n r_{n+1} + q_{n-1}}.$$

Entonces

$$\begin{aligned} r_{n+1}q_n\alpha + q_{n-1}\alpha &= r_{n+1}p_n + p_{n-1} \\ r_{n+1}(q_n\alpha - p_n) &= p_{n-1} - q_{n-1}\alpha, \end{aligned}$$

de donde

$$r_{n+1} = -\frac{q_{n-1}\alpha - p_{n-1}}{q_n\alpha - p_n} > 1.$$

De ello se deduce

$$|q\alpha - p| \geq |q_{n-1}\alpha - p_{n-1}| > |q_n\alpha - p_n|.$$

Q.e.d.

EJEMPLOS:

1. Mejor aproximación de $\sqrt{2}$.

$$\sqrt{2} = 1 + \left(\sqrt{2} - 1\right) = 1 + \frac{1}{2 + \left(\sqrt{2} - 1\right)},$$

entonces

$$\sqrt{2} = [1; \overline{2}].$$

De las fórmulas para p_n y q_n se tiene

$$\begin{array}{rcll} \frac{p_1}{q_1} & = & \frac{2\cdot 1+1}{2\cdot 1}=\frac{3}{2}, & \left|\sqrt{2}-\frac{3}{2}\right|<\frac{1}{4}=0,25 \\ \frac{p_2}{q_2} & = & \frac{2\cdot 3+1}{2\cdot 2+1}=\frac{7}{5}, & \left|\sqrt{2}-\frac{7}{5}\right|<\frac{1}{25}=0,04 \\ \frac{p_3}{q_3} & = & \frac{2\cdot 7+3}{2\cdot 5+2}=\frac{17}{12}, & \left|\sqrt{2}-\frac{17}{12}\right|<\frac{1}{144}=0,007 \\ \cdots & \cdots & \cdots & \end{array}$$

2. Mejor aproximación de π.

   La ley de formación general de la fracción continua de π no es conocida. Pero si se utiliza un número suficiente de cifras del desarrollo decimal de π, se pueden determinar los primeros elementos de la fracción continua. Así se tiene

   $$\pi = [1; 7, 15, 1, 292, \ldots].$$

   De las fórmulas para p_n y q_n se tiene

   $$\begin{array}{rcll} \frac{p_1}{q_1} & = & \frac{7\cdot 3+1}{7\cdot 1}=\frac{22}{7}, & \left|\pi-\frac{22}{7}\right|<\frac{1}{49}=0,021 \\ \frac{p_2}{q_2} & = & \frac{15\cdot 22+3}{15\cdot 7+1}=\frac{333}{106}, & \left|\pi-\frac{333}{106}\right|<\frac{1}{106^2}=0,00009 \\ \frac{p_3}{q_3} & = & \frac{1\cdot 333+22}{1\cdot 106+7}=\frac{355}{113}, & \left|\pi-\frac{355}{113}\right|<\frac{1}{113^2}=0,00008 \\ \cdots & \cdots & \cdots & \end{array}$$

   Aquí es notable que la primera y tercera aproximaciones dan un error mucho mejor que el teórico, pues

   $$\begin{aligned} \pi-\frac{22}{7} &< -0,001 \\ \pi-\frac{355}{113} &< -0,0000002. \end{aligned}$$

Se estudian a continuación las aproximaciones de α por $\frac{p}{q}$ con

$$\left|\alpha-\frac{p}{q}\right|<\frac{c}{qn},$$

con c constante independiente de $\frac{p}{q}$ y $n\in\mathbb{N}$.

Definición 6.2.1

*α se dice **aproximable en el orden n por números racionales** $\frac{p}{q}$ ($n\in\mathbb{N}$) si existe una constante $c=c(\alpha)$ que solo depende de α tal que*

$$\left|\alpha-\frac{p}{q}\right|<\frac{c(\alpha)}{qn}$$

tiene infinitas soluciones $\frac{p}{q}\in\mathbb{Q}$.

TEOREMA 6.2.3

Todo número racional es aproximable en el orden 1 y no lo es en ningún orden superior.

Demostración: Sea $\alpha = \frac{a}{b}$ con $(a, b) = 1$. Entonces la ecuación diofántica lineal $aq - bp = 1$ tiene infinitas soluciones $p; q$ con $(p, q) = 1$. Así es

$$\frac{a}{b} - \frac{p}{q} = \frac{1}{bq},$$

por lo que

$$\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{2}{q}$$

tiene infinitas soluciones y $\alpha = \frac{a}{b}$ es aproximable en el orden 1.

Si $b, q > 0$ y $\frac{a}{b} \neq \frac{p}{q}$, entonces

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} = \frac{1}{bq}.$$

Pero la aproximabilidad en el orden 2 exige que $q < bc$, lo que sucede sólo un número finito de veces. Luego, α no es aproximable en el orden 2. **Q.e.d.**

TEOREMA 6.2.4 *Todo número irracional es aproximable en el orden 2.*

Demostración: Sea α irracional. Entonces α tiene un desarrollo en fracción continua infinita. Por el teorema 6.1.6 los $\frac{p_n}{q_n}$ son las aproximaciones buscadas. **Q.e.d.**

TEOREMA 6.2.5

Si α es una irracionalidad cuadrática, entonces α no es aproximable en un orden superior a 2.

Demostración: Sea $\alpha = [a_0; a_1, a_2, \ldots]$ una irracionalidad cuadrática. Entonces α tiene un desarrollo en fracción continua periódica y los denominadores parciales a_n son acotados. Sea $0 < a_n < M$ para todo $n > 1$. Hacemos

$$\alpha = [a_0; a_1, a_2, \ldots, a_n, r_{n+1}].$$

Por el teorema 6.1.5 es

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(r_{n+1}q_n + q_{n+1})}.$$

Pero

$$r_{n+1} = a_{n+1} + \frac{1}{r_{n+2}} < a_{n+1} + 1,$$

de donde

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{q_n((a_{n+1}+1)q_n + q_{n+1})} > \frac{1}{(M+2)q_n^2}.$$

Sea ahora $\frac{p}{q}$ una aproximación con $q > 1$ y $q_{n+1} < q \leq q_n$. Como $\frac{p_n}{q_n}$ es la mejor aproximación (Lagrange) se cumple

$$\left|\alpha - \frac{p}{q}\right| > \left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{(M+2)q^2}\left(\frac{q}{q_n}\right)^2 > \frac{1}{(M+2)q^2}\left(\frac{q_{n-1}}{q_n}\right)^2.$$

Pero $q_n = a_n q_{n-1} + q_{n-2}$, de donde

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{(M+2)q^2}\frac{1}{\left(a_n + \frac{q_{n-2}}{q_{n-1}}\right)^2} > \frac{1}{(M+2)^3 q^2}.$$

Pero la aproximabilidad en el orden 3 exige que $q < (M+2)^3 c$, lo que sucede sólo un número finito de veces. Luego, α no es aproximable en el orden 3. **Q.e.d.**

6.3. Números algebraicos

DEFINICIÓN 6.3.1

*Un número real α se llama **número algebraico de grado** n si α es raíz de la ecuación de grado n*

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0, \tag{6.8}$$

con $a_i \in \mathbb{Z}$ para $i = 0, \ldots, n$ y $a_n \neq 0$ y α no es raíz de otra ecuación de grado inferior.

- Los números racionales son números algebraicos de grado 1.
- Las irracionalidades cuadráticas son números algebraicos de grado 2.
- Si p es primo, entonces $\sqrt[n]{p}$ es un número algebraico de grado n.

TEOREMA 6.3.1 *El conjunto de todos los números algebraicos es numerable.*

Demostración: Sea

$$H = n + |a_0| + |a_1| + \ldots + |a_{n-1}| + |a_n|$$

la *altura* de (6.8).

Es obvio que el valor mínimo de H es 2. También es obvio que sólo hay un número finito de ecuaciones del tipo (6.8) con altura fija H. Sean ellas

$$E_{H,1}, E_{H,2}, \ldots, E_{H,K_H}.$$

Ordenándolas en una sucesión se tiene

$$E_{2,1}, E_{2,2}, \ldots, E_{2,K_2}, E_{3,1}, \ldots, E_{3,K_3}, \ldots$$

El conjunto de estas ecuaciones es numerable. Pero todo número algebraico se corresponde al menos a una de esas ecuaciones y cada una de ellas tiene un número finito de soluciones, entonces el conjunto de los números algebraicos es numerable.

Q.e.d.

TEOREMA 6.3.2 ***Liouville***

Un número algebraico de grado n no es aproximable en un orden mayor que n.

Demostración: Basta demostrar que para todo par de enteros $p.q$ con $q > 0$ existe una constante K con

$$\left|\alpha - \frac{p}{q}\right| > \frac{K}{q^n},$$

si α es un número real algebraico de grado n.

Sea

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad \text{y} \qquad f(\alpha) = 0.$$

Entonces

$$f(x) = (x - \alpha) f_1(x) \qquad \text{con} \qquad f_1(\alpha) \neq 0,$$

por lo que existe $\delta > 0$ con

$$f_1(\alpha) \neq 0 \qquad \text{para} \qquad \alpha - \delta \leq x \leq \alpha + \delta.$$

Sea $|f_1(x)| < M$ para $x \in [\alpha - \delta, \alpha + \delta]$ y sea $\frac{p}{q}$ una aproximación de α $(q > 0)$ con

$$\left|\alpha - \frac{p}{q}\right| < \delta.$$

Entonces es

$$\begin{aligned} \left|\alpha - \frac{p}{q}\right| &= \left|\frac{f\left(\frac{p}{q}\right)}{f_1\left(\frac{p}{q}\right)}\right| = \frac{|a_n p^n + a_{n-1}p^{n-1}q^n + \ldots + a_1 p q^{n-1} x + a_0 q^n|}{\left|f_1\left(\frac{p}{q}\right)\right| q^n} \\ &> \frac{1}{M q^n} = \frac{K}{q^n} \end{aligned}$$

Q.e.d.

6.4. Números trascendentes

DEFINICIÓN 6.4.1 *4.5*

Un número real α que no es algebraico, se llama ***trascendente****.*

Del teorema de Louville[2] se deduce la existencia de números trascendentes, por eso es tan importante.

TEOREMA 6.4.1 ***Liouville***

El número

$$\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \ldots + \frac{1}{10^{n!}} + \ldots$$

es trascendente.

Demostración: Sea

$$\alpha_n = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \ldots + \frac{1}{10^{n!}} = \frac{p}{q}$$

con $q = 10^{n!}$. Entonces

$$0 < \alpha - \frac{p}{q} = \alpha - \alpha_n = \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \ldots < \frac{2}{10^{(n+1)!}} = \frac{2}{q^{n+1}}.$$

Luego, para todo valor de n mayor que un natural N, se cumple que la inecuación

$$0 < \alpha - \frac{p}{q} < \frac{2}{q^N}$$

tiene infinitas soluciones, por lo que α es aproximable en todo orden N y por tanto no es algebraico. **Q.e.d.**

Del Análisis Matemático es conocido el Teorema de Cantor que plantea que el conjunto de los números reales no es numerable. De él es posible deducir fácilmente el siguiente teorema.

TEOREMA 6.4.2 *El conjunto de los números trascendentes es no numerable.*

[2]Joseph Louville(1809-1882)

6.5. La irracionalidad de e y π

TEOREMA 6.5.1 *El número e es irracional.*

Demostración: (Variante sencilla de Fourier[3])

De los desarrollos en series de potencias se conoce que

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Supongamos que e es un número racional, entonces es $e = \frac{p}{q}$ con $(p, q) = 1$ y $p > 1$. Para $n \geq q$ se construye el número

$$\alpha = n! \left(e - \sum_{k=0}^{n} \frac{1}{k!} \right).$$

Como $e = \frac{p}{q}$ y $n \geq q$, entonces q y $k!$ dividen a $n!$ para todo $k \leq n$, por lo que α es un número entero.

Por otro lado es

$$\begin{aligned} \alpha &= n! \left(e - \sum_{k=0}^{n} \frac{1}{k!} \right) = n! \left(\sum_{k=n+1}^{\infty} \frac{1}{k!} \right) \\ &= n! \left(\sum_{k=1}^{\infty} \frac{1}{(n+k)!} \right) = n! \left(\sum_{k=1}^{\infty} \frac{1}{n!(n+1) \cdot \ldots \cdot (n+k)} \right) \\ &= \sum_{k=1}^{\infty} \frac{1}{(n+1) \cdot \ldots \cdot (n+k)}. \end{aligned}$$

Pero $\frac{1}{(n+1)\cdot\ldots\cdot(n+k)} < \frac{1}{(n+1)^{k-n}}$, de donde

$$0 < \alpha < \sum_{k=1}^{\infty} \frac{1}{(n+1)^{k-n}} < 1,$$

lo cual es imposible, pues α es un número entero. Entonces e es un número irracional.
Q.e.d.

TEOREMA 6.5.2 *El número π es irracional.*

[3] Jean Baptiste Joseph Fourier (1768-1830)

Demostración: (Variante de Van Niven[4])

Supongamos que π es un número racional, entonces es $\pi = \frac{p}{q}$ con $(p, q) = 1$.

Definimos las funciones

$$f(x) = \frac{x^n(p - qx)^n}{n!} \qquad \text{y} \qquad F(x) = f(x) - \sum_{k=1}^{n}(-1)^k f^{(2k)}(x).$$

Entonces es

$$f(x) = \frac{1}{n!}\sum_{i=n}^{2n} c_i x^i$$

con $c_i \in \mathbb{Z}$ para $i = n, \ldots, 2n$. Derivando se tiene

$$f^{(k)}(x) = \frac{1}{n!}\sum_{i=n}^{2n} c_i i(i-1)\cdot \ldots \cdot (i-k)x^{i-k},$$

de donde

$$f^{(k)}(0) = \begin{cases} 0 & \text{si} \quad k < n \quad \text{ó} \quad k > 2n, \\ c_k & \text{si} \quad n \leq k \leq 2n, \end{cases}$$

y por tanto $f^{(k)}(0)$ es entero para todo valor de k.

Además

$$\begin{aligned} f(\pi - x) &= f\left(\frac{p}{q} - x\right) = \frac{\left(\frac{p}{q} - x\right)^n \left(p - q\left(\frac{p}{q} - x\right)\right)^n}{n!} \\ &= \frac{\frac{(p-qx)^n}{q^n}(qx)^n}{n!} = \frac{(p - qx)^n x^n}{n!}. \end{aligned}$$

Es decir, $f(\pi - x) = f(x)$ y por tanto $f^{(k)}(\pi)$ es entero para todo valor de k.

Por otra parte es

$$F(0) = f(0) - \sum_{k=1}^{n}(-1)^k f^{(2k)}(0),$$

y por tanto $F(0)$ es entero. De manera análoga se demuestra que $F(\pi)$ es entero.

Ahora, derivando la función $F'(x)\operatorname{sen} x - F(x)\cos x$ se obtiene

$$\frac{d}{dx}(F'(x)\operatorname{sen} x - F(x)\cos x) = \operatorname{sen} x(F''(x) + F(x)).$$

[4]Ivan Morton Niven(1915-1999)

Pero

$$\begin{aligned} F''(x)+F(x) &= f''(x)+\sum_{k=1}^{n}(-1)^k f^{(2k+2)}(x)+f(x)+\sum_{k=1}^{n}(-1)^k f^{(2k)}(x) \\ &= f''(x)+f(x)+\sum_{k=1}^{n}(-1)^k f^{(2k+2)}(x) \\ &\quad -f''(x)+\sum_{k=1}^{n}(-1)^{k+1} f^{(2k+2)}(x) = f(x). \end{aligned}$$

Entonces es

$$\frac{d}{dx}(F'(x)\operatorname{sen} x - F(x)\cos x) = f(x)\operatorname{sen} x.$$

Integrando $f(x)\operatorname{sen} x$ se tiene

$$\int_0^\pi f(x)\operatorname{sen} x\ dx = (F'(x)\operatorname{sen} x - F(x)\cos x)\ |_0^\pi = F(\pi)-F(0)\in\mathbb{Z}.$$

Por otra parte, es

$$0 < f(x)\operatorname{sen} x \le f(x) < \frac{\pi^n p^n}{n!}$$

para $0<x<\pi$, de donde para n suficientemente grande se obtiene

$$0 < \int_0^\pi f(x)\operatorname{sen} x\ dx < \frac{\pi^{n+1}p^n}{n!} < 1,$$

lo cual es imposible, pues

$$\int_0^\pi f(x)\operatorname{sen} x\ dx \in \mathbb{Z}.$$

Entonces π es racional. **Q.e.d.**

6.6. La trascendencia de e y π

LEMA 6.6.1

Sean las funciones

$$f(x)=\sum_{i=0}^{n} a_i x^i$$

con $a_1\in\mathbb{Z}$ *para* $i=1\ldots n$ *y*

$$F(x)=\sum_{k=0}^{n} f^{(k)}(x).$$

Entonces es

$$|F(0)e^x - F(x)| \le e^{|x|}\sum_{i=0}^{n}|a_i||x|^i.$$

Demostración:

$$\begin{aligned} F(x) &= \sum_{k=0}^{n}\sum_{i=k}^{n} a_i \frac{i!}{(i-k)!}x^{i-k} \\ &= \sum_{i=0}^{n} i!a_i \left(\sum_{k=0}^{i} \frac{x^{i-k}}{(i-k)!}\right) \\ &= \sum_{i=0}^{n} i!a_i \left(\sum_{k=0}^{i} \frac{x^{k}}{k!}\right). \end{aligned}$$

Entonces es

$$F(0) = \sum_{i=0}^{n} i!a_i,$$

por lo que (desarrollando la exponencial en series de potencias) se tiene

$$\begin{aligned} |F(0)e^x - F(x)| &= \left|\sum_{i=0}^{n} i!a_i \left(\sum_{k=0}^{\infty} \frac{x^k}{k!}\right) - \sum_{i=0}^{n} i!a_i \left(\sum_{k=0}^{i} \frac{x^k}{k!}\right)\right| \\ &= \left|\sum_{i=0}^{n} i!a_i \left(\sum_{k=i+1}^{\infty} \frac{x^k}{k!}\right)\right| \\ &\leq \sum_{i=0}^{n} |a_i| \left(\sum_{k=i+1}^{\infty} \frac{|x|^k}{(k-i)!}\right). \end{aligned}$$

Sumando y restando i al exponente de la x en esta última expresión se obtiene finalmente la tesis del lema. **Q.e.d.**

TEOREMA 6.6.1 *El número e es trascendente.*

Demostración: (Variante de Hermite[5])

Queremos demostrar que para todo polinomio $P(x) = \sum_{i=0}^{n} c_i x^i$ con $c_i \in \mathbb{Z}$ para $i = 1, \ldots, n$ y $c_n \neq 0$, se cumple $P(e) \neq 0$. Sea p primo con $p > \text{máx}\{|c_0|, m\}$. Construimos las funciones

$$f(x) = \frac{x^{p-1}}{(p-1)!}\prod_{k=1}^{m}(k-x)^p = \sum_{j=0}^{n} a_j x^j \qquad \text{y} \qquad F(x) = \sum_{k=0}^{n} f^{(k)}(x).$$

Hacemos

$$F(0)P(e) = A_1 + A_2$$

[5]Charles Hermite (1822-1901)

con

$$A_1 = \sum_{i=0}^{m} c_i F(i) \qquad \text{y} \qquad A_2 = \sum_{i=0}^{m} c_i (F(0)e^i - F(i)).$$

De manera análoga a la demostración de la irracionalidad de π se obtiene

$$A_1 = \sum_{i=0}^{m} c_i \left(\sum_{k=0}^{n} f^{(k)}(i) \right) \in \mathbb{Z} \qquad \text{y} \qquad A_1 \equiv c_0 (m!)^p (mod\ p),$$

de donde, como $c_0 \neq 0$ y $p > \text{máx}\{|c_0|, m\}$, se deduce que $A_1 \neq 0$ y más aún, que $|A_1| \geq 1$.

Por otra parte, aplicando el lema anterior, es

$$\left| F(0)e^i - F(i) \right| \leq e^i \cdot \sum_{j=0}^{n} |a_j| i^j = e^i \frac{i^{p-1}}{(p-1)!} \prod_{k=1}^{n} (k+i)^p \longrightarrow 0,$$

cuando $p \to \infty$, por lo que $|A_2| < 1/2$ para p suficientemente grande.

Entonces $F(0)P(e) = A_1 + A_2 \neq 0$, pues $|A_1| \geq 1$ y $|A_2| < 1/2$ y por tanto es $P(e) \neq 0$, de donde se deduce la trascendencia de e. **Q.e.d.**

La demostración de la trascendencia de π es aún menos elemental, pues en ella se utiliza el hecho de que $e^{\imath\pi} = -1$, siendo $\imath = \sqrt{-1}$. Nótese además que si el número x es algebraico, entonces existen enteros d_k no todos nulos tales que

$$\sum_{k=0}^{m} d_k x^k = 0.$$

Sustituyendo en esta expresión el número complejo $y = ix$ se obtiene

$$\begin{aligned} d_0 - \imath d_1 y + d_2 y^2 + \imath d_3 y^3 + d_4 y^4 - \ldots &= 0 \\ (d_0 - d_2 y^2 + d_4 y^4 - \ldots) + \imath(d_1 - d_3 y + d_5 y^5 - \ldots) &= 0, \end{aligned}$$

por lo que $y = ix$ es también un número algebraico.

TEOREMA 6.6.2 *El número π es trascendente.*

Demostración: (Variante de Lindemann[6])

Supongamos que π es un número algebraico, entonces $i\pi$ es también algebraico y raíz de una ecuación

$$\sum_{k=0}^{m} c_k x^k = 0$$

[6]Carl Louis Ferdinand von Lindemann (1852-1939)

con $c_k \in \mathbb{Z}$ para $k = 0, \ldots, m$ y $c_m \neq 0$.

Denotemos por $x_1, x_2, \ldots, x_m$ a las raíces de la ecuación anterior, entre las que se encuentran $i\pi$ y $-i\pi$. Como $e^{i\pi} = -1$, se cumple

$$\prod_{k=1}^{m}(1 + e^x k) = 1 + \sum_{i=1}^{2^m-1} e^{y_i} = 0 \tag{6.9}$$

con

$$y_i \in \{x_1, \ldots, x_m, x_1 + x_2, x_1 + x_3, \ldots, x_1 + x_m, \ldots, x_1 + x_2 + \ldots + x_m\}$$

Entonces al menos un $y_i = 0$, por ejemplo, el correspondiente a la suma de las raíces $i\pi$ y $-i\pi$. Luego, podemos suponer que

$$\begin{aligned} y_i &\neq 0 \quad \text{para} \quad i = 1, \ldots, n \\ y_i &= 0 \quad \text{para} \quad i = n+1, \ldots, 2^m - 1. \end{aligned}$$

Sea $q = 2^m - n$, entonces por (6.9) es

$$q + \sum_{i=1}^{n} e^{y_i} = 0. \tag{6.10}$$

En la representación

$$g_n \sum_{i=1}^{n}(x - y_i) = \sum_{r=0}^{n} g_r x^r$$

para $0 \leq r \leq n-1$ los g_r son (obviando el signo) las funciones simétricas elementales en $y_1, y_2, \ldots, y_n$, por lo que son también polinomios simétricos en $y_1, y_2, \ldots, y_n$. Aplicando el teorema fundamental para polinomios simétricos, se deduce que ellos son también polinomios simétricos en $x_1, x_2, \ldots, x_m$, por lo cual son enteros y naturalmente es $g_0 \neq 0$ y $g_n \neq 0$.

Aplicaremos ahora otra vez el lema estudiado anteriormente. Sea p un número primo con $p > \text{máx}\{q, |g_0|, |g_n|\}$ y sean

$$f(x) = \frac{g_b^{pn-1}}{(p-1)!} x^{p-1}(g_0 + g_1 x + \ldots + g_n x^n)^p \quad \text{y} \quad F(x) = \sum_{k=0}^{n} f^{(k)}(x).$$

Para el número

$$A = qF(0) + \sum_{i=1}^{n} F(y_i) \tag{6.11}$$

aplicando el lema y (6.10) se obtiene

$$|A| = \left| \sum_{i=1}^{n} F(y_i) - e^{y_i} F(0) \right| \leq \sum_{i=1}^{n} e^{|y_i|} h(y_i)$$

con

$$h(x) = \frac{|g_n|^{pn-1}}{(p-1)!}|x|^{p-1}(|g_0| + |g_1||x| + \ldots + |g_n||x|^n)^p.$$

Haciendo $y = \text{máx}\{|y_1|, \ldots, |y_n|\}$ se obtiene

$$|A| \leq ne^y h(y).$$

Para p grande, $h(y)$ se hace tan pequeño como se quiera y se puede alcanzar $|A| < 1$.

Demostraremos ahora que A es entero y no es divisible por p, alcanzando así una contradicción. En la expresión (6.11) de A es $qF(0)$ un número entero que no es divisible por p, pues

$$qF(0) \equiv qg_n^{pn-1}(mod\ p) \quad \text{y} \quad p > \text{máx}\{q, |g_0|, |q_n|\}.$$

O sea, debemos demostrar que

$$\sum_{i=1}^{n} F(y_i)$$

es un entero divisible por p.

Como

$$g_0 + g_1x + \ldots + g_nx^n = g_n(x - y_1)(x - y_2)\ldots(x - y_n),$$

entonces

$$f(x) = \frac{(g_nx)^{p-1}}{(p-1)!}(g_nx - g_ny_1)^p(g_nx - g_ny_2)^p \ldots (g_nx - g_ny_n)^p.$$

Desarrollando en potencias de $(g_nx - g_ny_i)$ para $1 \leq i \leq n$ se tiene

$$f(x) = \sum_{k=p}^{np+p-1} \frac{a_{ik}}{k!}(g_nx - g_ny_i)^k,$$

donde los a_{ik} son polinomios en $g_ny_1, g_ny_2, \ldots, g_ny_n$ con coeficientes enteros divisibles por p. Ellos representan además funciones simétricas de las variables

$$y_1, y_2, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n$$

y se cumple

$$F(y_i) = \sum_{k=p}^{np+p-1} a_{ik}g_n^k.$$

Por lo que

$$\sum_{i=1}^{n} F(y_i) = \sum_{k=p}^{np+p-1} g_n^k \sum_{i=1}^{n} a_{ik},$$

siendo

$$\sum_{i=1}^{n} a_{ik}$$

funciones simétricas enteras con coeficientes enteros divisibles por p. Como a los términos $g_n y_1, g_n y_2, \ldots, g_n y_n$, corresponde la ecuación

$$g_0 g_n^{n-1} + g_1 g_n^{n-2} x + \ldots + g_{n-2} x^{n-1} + x^n = 0,$$

cuyo mayor coeficiente es 1, entonces

$$\sum_{i=1}^{n} F(y_i)$$

es un número entero divisible por p.

Entonces A es entero y no es divisible por p, por lo que $A \neq 0$. Pero eso es imposible, pues $|A| < 1$. Luego, π es trascendente. **Q.e.d.**

6.7. Ejercicios del capítulo

1. Demuestre que si el número natural N no es un cuadrado, entonces $\sqrt{N}$ es irracional.

2. Demuestre que si n, m son números naturales diferentes con $(n, m) = 1$, entonces $\log_n m$ es irracional.

3. Sea $x \in \mathbb{R}$ raíz de la ecuación

   $$x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0,$$

   con $a_i \in \mathbb{Z}$. Demuestre que x es entero o irracional.

4. Determine las tres primeras mejores aproximaciones de $\sqrt{3}$, $\sqrt{5}$ y $\sqrt{7}$.

5. Calcule $[2; \overline{1, 1, 3}]$, $[6; \overline{3, 12}]$ y $[4; \overline{2, 8}]$.

6. Para números naturales n demuestre que

   $$\sqrt{n^2 + 1} = [n; \overline{2n}] \qquad \text{y} \qquad \sqrt{n^2 + 2} = [n; \overline{n, 2n}].$$

7. Exprese los siguientes números racionales como fracciones continuas simples finitas

   (a) $-\frac{19}{51}$, (b) $\frac{187}{57}$, (c) $-\frac{71}{55}$, (d) $-\frac{118}{303}$.

8. Determine los números racionales representados por las siguientes fracciones continuas simples finitas

   (a) $[-2; 2, 4, 6, 8]$, (b) $[4; 2, 1, 3, 1, 2, 4]$, (c) $[0; 1, 2, 3, 4, 3, 2, 1]$.

9. Si $r = [a_0; a_1, \ldots, a_n]$ con $r > 1$, demuestre que

$$\frac{1}{r} = [0; a_0, a_1, \ldots, a_n].$$

10. Represente las siguientes fracciones continuas simples finitas en forma equivalente, pero con un número impar de denominadores parciales.

    (a) $[0; 3, 1, 2, 3]$, (b) $[-1; 2, 1, 6, 1]$, (c) $[2; 3, 1, 2, 1, 1, 1]$.

11. Halle las k-ésimas aproximaciones de las siguientes fracciones continuas simples finitas.

    (a) $[1; 2, 3, 2, 1]$, (b) $[-3; 1, 1, 1, 1, 3]$, (c) $[0; 2, 4, 1, 8, 2]$.

12. *a*) Si $C_n = \frac{p_n}{q_n}$ es la n-ésima aproximación de la fracción continua simple $[1; 2, 3, 4, \ldots, n, n+1]$, demuestre que

$$p_n = np_{n-1} + np_{n-2} + (n-1)p_{n-3} + \ldots + 3p_1 + 2p_0 + (p_0 + 1).$$

    (Sugerencia: Sume las relaciones $p_0 = 1$, $p_1 = 3$, $p_k = (k+1)p_{k-1} + p_{k-2}$ para $k = 2, \ldots, n$).

    b) Ejemplifique el inciso a) calculando los numeradores p_k de $[1; 2, 3, 4, 5]$.

13. Calcule p_k, q_k y C_k $(k = 1, \ldots, 8)$ para las siguientes fracciones continuas simples finitas y compruebe que las k-ésimas aproximaciones constituyen aproximaciones de las números irracionales entre paréntesis.

    a) $[1; 2, 2, 2, 2, 2, 2, 2, 2]$ $(\sqrt{2})$
    b) $[1; 1, 2, 1, 2, 1, 2, 1, 2]$ $(\sqrt{3})$
    c) $[2; 4, 4, 4, 4, 4, 4, 4, 4]$ $(\sqrt{5})$
    d) $[2; 2, 4, 2, 4, 2, 4, 2, 4]$ $(\sqrt{6})$
    e) $[2; 1, 1, 1, 4, 1, 1, 1, 4]$ $(\sqrt{7})$

14. Si $C_k = \frac{p_k}{q_k}$ es la k-ésima aproximación de la fracción continua simple $[a_0; a_1, \ldots, a_n]$, compruebe que

$$q_k \geq 2^{\frac{k-1}{2}} \qquad (2 \leq k \leq n).$$

    (Sugerencia: Observe que $q_k = a_k q_{k-1} + q_{k-2} \geq 2q_{k-2}$.)

15. Encuentre las fracciones continuas simples finitas que representan los números $3,1416$ y $3,14159$.

16. Si $C_k = \frac{p_k}{q_k}$ es la k-ésima aproximación de la fracción continua simple $[a_0; a_1, \ldots, a_n]$ con $a_0 > 0$, demuestre que

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0]$$

y

$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \ldots, a_2, a_1].$$

(Sugerencia: Observe que

$$\frac{p_k}{p_{k-1}} = a_k + \frac{p_{k-2}}{p_{k-1}} = a_k + \frac{1}{\frac{p_{k-1}}{p_{k-2}}}$$

en el primer caso.)

17. Resuelva las siguientes ecuaciones diofánticas por el método de las fracciones continuas

    a) $19x + 51y = 1$,

    b) $364x + 227y = 1$,

    c) $18x + 5y = 24$,

    d) $158x - 57y = 1$.

18. Calcule las siguientes fracciones continuas infinitas

    (a) $[\overline{2;3}]$, (b) $[0;\overline{1,2,3}]$,
    (c) $[2;\overline{1,2,1}]$, (d) $[1;2,\overline{3,1}]$,
    (e) $[1;2,1,\overline{2\,1\,2}]$.

19. Demuestre que si el número irracional x se representa por la fracción continua infinita $[a_0; a_1.a_2, \ldots]$, entonces $\frac{1}{x}$ tiene el desarrollo $[0; a_0, a_1.a_2, \ldots]$. Utilice ese resultado para hallar el valor de $[0; 1, 1, 1, \ldots] = [0; \overline{1}]$.

20. Calcule $[1; 2, \overline{1}]$ y $[1; 2, 3, \overline{1}]$

21. Determine la representación en fracciones de continuas de los siguientes números irracionales

    (a) $\sqrt{5}$, (b) $\sqrt{5}$, (c) $\frac{1+\sqrt{13}}{2}$
    (d) $\frac{5+\sqrt{37}}{4}$, (e) $\frac{11+\sqrt{30}}{13}$.

22. *a*) Para todo entero positive n, demuestre que $\sqrt{n^2+1} = [n; \overline{2n}]$, $\sqrt{n^2+2} = [n; \overline{n, 2n}]$ y $\sqrt{n^2+2n} = [n; \overline{1, 2n}]$. (Sugerencia: Note que

$$n + \sqrt{n^2+1} = 2n + (\sqrt{n^2+1} - n) = 2n + \frac{1}{n + \sqrt{n^2+1}}.\Big)$$

b) Su a y b son enteros positivos, demuestre que la desigualdad $0 < \frac{a}{b} < \frac{87}{32}$ implica que $b \geq 39$.

23. Demuestre que de dos k-ésimas aproximaciones consecutivas del número irracional x, al menos una satisface la desigualdad

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2}.$$

(Sugerencia: Como x está entre dos k-ésimas aproximaciones consecutivas , se cumple

$$\frac{1}{q_n q_{n+1}} - \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \left| x - \frac{p_{n+1}}{q_{n+1}} \right| + \left| x - \frac{p_n}{q_n} \right|.$$

Ahora utilice el absurdo.)

24. Dada la fracción continua infinita $[1; 3, 1, 5, 1, 7, 1, 9, \ldots]$, halle la mejor aproximación racional $\frac{a}{b}$ con

(a) denominador $b < 25$, (b) denominador $b < 225$

25. Demuestre primero que

$$\left| \frac{1+\sqrt{10}}{3} - \frac{18}{13} \right| < \frac{1}{2 \cdot 13^2},$$

y verifique luego que $\frac{18}{13}$ es una k-ésima aproximación de $\frac{1+\sqrt{10}}{3}$.

26. Un famoso teorema de A.Hurwitz (1891) plantea que para todo número irracional x existen infinitos números racionales $\frac{a}{b}$ tales que

$$\left| x - \frac{a}{b} \right| < \frac{1}{\sqrt{5}b^2}.$$

Haciendo $x = \pi$ obtenga tres números racionales que cumplan esa desigualdad.

27. Asuma que la representación en fracción continua del número irracional π es periódica. Compruebe que x es de la forma $r + s\sqrt{d}$, donde r y $t \neq 0$ son números racionales y $d > 0$ es un entero no cuadrado.

28. Sea x un número irracional con aproximaciones $\frac{p_n}{q_n}$. Para todo $n \geq 0$ demuestre que

a) $\frac{1}{2q_nq_{n+1}} < \left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}}$

b) Las aproximaciones sucesivas se aproximan a x en el sentido de que

$$\left|x - \frac{p_n}{q_n}\right| < \left|x - \frac{p_{n-1}}{q_{n-1}}\right|.$$

(Sugerencia: Rescriba la relación

$$x = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}$$

como $x_{n+1}(xq_n - p_n) = -q_{n-1}\left(x - \frac{p_{n-1}}{q_{n-1}}\right)$.)

Capítulo 7

FUNCIONES ARITMÉTICAS

Aunque ya a lo largo de este texto se han definido algunas funciones aritméticas, se dedica aquí especial atención a las más utilizadas y a importantes operaciones entre ellas.

7.1. La multiplicación de Dirichlet de funciones aritméticas

Definición 7.1.1

*Una **función aritmética** es una función definida en $\mathbb{N}$ con valores reales o complejos.*

Definición 7.1.2

Si $f(n)$ y $g(n)$ son dos funciones aritméticas, entonces la función aritmética

$$h(n) = f(n) * g(n) = \sum_{t|n} f(t) g\left(\frac{n}{t}\right)$$

*define su **producto de Dirichlet**.*

Si t recorre los divisores de n, entonces $\frac{n}{t}$ representa al divisor complementario. Luego, también se puede escribir

$$f(n) * g(n) = \sum_{td=n} f(t) g(d).$$

PROPIEDADES

- La multiplicación de Dirichlet[1] es conmutativa.

  Demostración:

  $$f(n) * g(n) = \sum_{td|n} f(t)g(d) = \sum_{td|n} f(d)g(t) = g(n) * f(n).$$

  Q.e.d.

- La multiplicación de Dirichlet es asociativa.

  Demostración:

  $$\begin{aligned} f(n) * (g(n) * h(n)) &= f(n) * \sum_{t_1 t_2|n} g(t_1)h(t_2) = \sum_{td|n} f(d)g(t) = g(n) * f(n) \\ &= \sum_{t_3 d|n} f(t_3) \sum_{t_1 t_2 = d} g(t_1)h(t_2) \\ &= \sum_{t_1 t_2 t_3|n} f(t_3)g(t_1)h(t_2) = (f(n) * g(n)) * h(n). \end{aligned}$$

  Q.e.d.

- La multiplicación de Dirichlet tiene unidad.

  Demostración:

  $$\epsilon(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases},$$

  pues

  $$\epsilon(n) * f(n) = \sum_{t|n} f(t)\epsilon\left(\frac{n}{t}\right) = f(n).$$

  Q.e.d.

- La unidad de la multiplicación de Dirichlet es única en el conjunto de las funciones aritméticas que cumplen $f(1) \neq 0$.

  Demostración: Supongamos que existe $\epsilon_1(n)$ con $\epsilon_1(n) * f(n) = f(n)$ para toda funcióm aritmética f con $f(1) \neq 0$. Entonces

  $$(\epsilon(n) - \epsilon_1(n)) * f(n) = \sum_{t|n} (\epsilon(t) - \epsilon_1(t)) f\left(\frac{n}{t}\right) = 0.$$

[1] Peter Gustav Dirichlet (1805-1859)

Como $f(1) \neq 0$, de $(\epsilon(n) - \epsilon_1(n)) * f(n) = 0$ se deduce que $\epsilon(1) = \epsilon_1(1)$. Entonces, para $n = 2$, la relación

$$\sum_{t|2}(\epsilon(t) - \epsilon_1(t))f\left(\frac{2}{t}\right) = (\epsilon(1) - \epsilon_1(1))f(2) + (\epsilon(2) - \epsilon_1(2))f(1) = 0$$

implica que $\epsilon(2) = \epsilon_1(2)$. Finalmente, si $\epsilon(k) = \epsilon_1(k)$ para $k < n$, entonces, como $f(1) \neq 0$, se cumple $\epsilon(n) = \epsilon_1(n)$ para todo $n \in \mathbb{N}$. **Q.e.d.**

- $f(1) \neq 0$ implica que la ecuación $f(n) * x(n) = \epsilon(n)$ tiene solución única. La solución $x(n)$ de esta ecuación es la función inversa de $f(n)$ $(x(n) = f(n)^{-1})$.

  Demostración:

  $$\sum_{t|n} f\left(\frac{n}{t}\right) x(t) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases},$$

  de donde

  $$x(1) = \frac{1}{f(1)}.$$

  Para $n > 1$, se determina $x(n)$ recursivamente a partir de

  $$x(n) = -\frac{1}{f(1)} \sum_{t|n,\ t<n} f\left(\frac{n}{t}\right) x(t).$$

  Q.e.d.

El teorema siguiente resume estas propiedades.

Teorema 7.1.1

El conjunto de las funciones aritméticas $f(n)$ con $f(1) \neq 0$ constituye un grupo abeliano respecto a la multiplicación de Dirichlet.

Definición 7.1.3

Una función aritmética $f(n)$ no idénticamente nula se dice ***multiplicativa*** *si y*

$$f(nm) = f(n)f(m) \qquad para \quad (n, m) = 1.$$

$f(n)$ se dice ***totalmente multiplicativa*** *si*

$$f(nm) = f(n)f(m) \qquad para\ todos \quad n, m \in \mathbb{Z}.$$

Si $f(n)$ es multiplicativa, siempre se cumple $f(1) = 1$, pues, como existe m tal que $f(m) \neq 0$, entonces

$$f(1 \cdot m) = f(1)f(m) = f(m).$$

TEOREMA 7.1.2

Si $f(n), g(n)$ son funciones multiplicativas, también lo es $f(n) * g(n)$.

Demostración: Sea $n = n_1 n_2$ con $(n_1, n_2) = 1$. Entonces

$$f(n) * g(n) = f(n_1 n_2) * g(n_1 n_2) = \sum_{t | n_1 n_2} f(t) g\left(\frac{n_1 n_2}{t}\right).$$

Se descompone $t = t_1 t_2$ con $(t_1, t_2) = 1$ tal que $t_1 | n_1$ y $t_2 | n_2$. Entonces

$$\begin{aligned} f(n) * g(n) &= \sum_{t_1 | n_1} \sum_{t_2 | n_2} f(t_1) g\left(\frac{n_1}{t_1}\right) f(t_2) g\left(\frac{n_2}{t_2}\right) \\ &= (f(n_1) * g(n_1))(f(n_2) * g(n_2)). \end{aligned}$$ **Q.e.d.**

Nota: Si $f(n), g(n)$ son funciones totalmente multiplicativas, ello no implica que también lo sea $f(n) * g(n)$.

EJEMPLO: $f(n) = n$ es totalmente multiplicativa. Sea $h(n) = f(n) * f(n)$. Entonces $h(2) = f(2) * f(2) = f(1)f(2) + f(2)f(1) = 4$, con lo cual $h(2) * h(2) = 8$, pero

$$h(4) = f(1)f(4) + f(2)f(2) + f(4)f(1) = 12 \neq h(2) * h(2),$$

por lo que $h(n) = f(n) * f(n)$ no es totalmente multiplicativa.

DEFINICIÓN 7.1.4

*Sea k un número real cualquiera. Se definen las **funciones de divisores** a través de*

$$\sigma_k(n) = 1 * n^k = \sum_{t | n} t^k.$$

En particular

- $\sigma_0(n) = \tau(n)$ *describe el* ***número de divisores de*** n.
- $\sigma_1(n) = \sigma(n)$ *describe la* ***suma de los divisores de*** n.

- La función $\sigma_k(n)$ es multiplicativa, pues las funciones 1 y t^k lo son.
- Para $n = p^\nu$ con p primo es

$$\sigma_k(p^\nu) = 1 + p^k + p^{2k} + \ldots + p^{\nu k} = \begin{cases} \frac{p^{k(\nu+1)}-1}{p^k-1} & k \neq 0 \\ \nu + 1 & k = 0 \end{cases}$$

- Si $n = \prod_{i=1}^{r} p_i^{\nu_i}$, entonces

$$\sigma_k(n) = \begin{cases} \prod_{i=1}^{r} \frac{p_i^{k(\nu_i+1)}-1}{p_i^k-1} & k \neq 0 \\ \prod_{i=1}^{r} (\nu_i + 1) = \tau(n) & k = 0 \end{cases}$$

TEOREMA 7.1.3

Si $g(n)$ y $f(n) * g(n)$ son funciones multiplicativas, también lo es $f(n)$.

Demostración: Demostraremos que si $f(n)$ no es multiplicativa, entonces la función $h(n) = f(n) * g(n)$ no es multiplicativa. Sean $(n_1, n_2) = 1$, de modo que $f(n_1 n_2) \neq f(n_1) f(n_2)$ y que el producto sea minimal.

Si $n_1 n_2 = 1$, entonces es

$$h(1) = f(1) * g(1) = f(1) \neq 1,$$

por lo que $h(n)$ no es multiplicativa.

Si $n_1 n_2 > 1$, entonces para $(n_1', n_2') = 1$ con $n_1' n_2' < n_1 n_2$ se tiene

$$f(n_1' n_2') = f(n_1') f(n_2').$$

De aquí que

$$\begin{aligned} h(n_1 n_2) &= \sum_{t_1 | n_1} \sum_{t_2 | n_2} f(t_1 t_2) g\left(\frac{n_1 n_2}{t_1 t_2}\right) + f(n_1 n_2) \\ &= \sum_{t_1 | n_1} \sum_{t_2 | n_2} f(t_1) f(t_2) g\left(\frac{n_1}{t_1}\right) g\left(\frac{n_2}{t_2}\right) - f(n_1) f(n_2) + f(n_1 n_2) \\ &= h(n_1) h(n_2) - f(n_1) f(n_2) + f(n_1 n_2) \neq h(n_1) h(n_2), \end{aligned}$$

pues $f(n_1 n_2) - f(n_1) f(n_2) > 0$. Luego $h(n)$ no es multiplicativa. **Q.e.d.**

DEFINICIÓN 7.1.5

*La función inversa de $f(n) \equiv 1$ se conoce como **función μ de Möbius**, es decir, $1 * \mu(n) = \epsilon(n)$ y se cumple*

$$\sum_{t | n} \mu(t) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

- La función de Möbius[2] $\mu(n)$ es multiplicativa, pues las funciones $\epsilon(n)$ y $f(n) \equiv 1$ lo son.
- Para $n = p^\nu$ con p primo es

  $$\mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^\nu) = 0.$$

  Pero $\mu(1) = 1$, de donde

  $$\mu(p^\nu) = \begin{cases} -1 & \nu = 1 \\ 0 & \nu > 1 \end{cases}$$

[2] August Möbius (1790-1868)

- Si $n = \prod_{i=1}^{r} p_i^{\nu_i}$, entonces

$$\mu(n) = \begin{cases} (-1)^r & \nu_1 = \ldots = \nu_r = 1 \\ 0 & \text{en otro caso} \end{cases}.$$

La siguiente es entonces una definición equivalente de la función de Möbius.

Para un entero positivo n se determina la función de Möbius μ por la fórmula

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & p^2 | n \text{ para cierto primo } p \\ (-1)^r & n = p_1 p_2 \cdots p_r \text{ para primos distintos } p_i \end{cases}.$$

La definición anterior afirma que $\mu(n) = 0$ si n no es libre de cuadrados, mientras que $\mu(n) = (-1)^r$ si n es libre de cuadrados con r factores primos. Por ejemplo,

$$\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1.$$

Los primeros valores de μ son

$$\mu(1) = 1, \quad \mu(2) = -1, \quad \mu(3) = -1, \quad \mu(4) = 0, \quad \mu(5) = -1, \quad \mu(6) = 1, \ldots$$

Si p es primo es claro que $\mu(p) = -1$, mientras que $\mu(p^k) = 0$ para $k \geq 2$.

Teorema 7.1.4

Si $g(n)$ es totalmente multiplicativa, entonces $g(n)^{-1} = \mu(n)g(n)$.

Demostración:

$$\begin{aligned} (\mu(n)g(n)) * g(n) &= \sum_{t|n} \mu(t)g(t)g\left(\frac{n}{t}\right) = g(n)\sum_{t|n}\mu(t) \\ &= \begin{cases} g(1)\cdot 1 & n = 1 \\ g(n)\cdot 0 & n > 1 \end{cases} \\ &= \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases} = \epsilon(n). \end{aligned}$$

Q.e.d.

De este teorema se deduce directamente el siguiente.

Teorema 7.1.5

Si $g(n)$ es totalmente multiplicativa, entonces

$$F(n) = f(n) * g(n) \qquad \Leftrightarrow \qquad f(n) = F(n) * (\mu(n)g(n)).$$

Consideremos $F(n) = f(n) * g(n)$ de modo que una de las dos funciones $f(n)$ o $F(n)$ es multiplicativa. Por los teoremas 7.1.2 y 7.1.3 la otra función ($F(n)$ o $f(n)$) es multiplicativa. Entonces basta calcular $f(n) = F(n) * (\mu(n)g(n))$ para $n = p^\nu$. Se cumple

$$f(p^\nu) = \sum_{t|p^\nu} \mu(t)g(t)F\left(\frac{p^\nu}{t}\right) = F(p^\nu) - g(p)F(p^{\nu-1}).$$

Si $n = \prod_{i=1}^{r} p_i^{\nu_i}$, entonces

$$f(n) = \prod_{i=1}^{r} \left(F(p_i^{\nu_i}) - g(p_i)F(p_i^{\nu_i-1})\right).$$

El siguiente teorema muestra la gran importancia de la función de Möbius.

TEOREMA 7.1.6 ***Fórmula de inversión de Möbius***

Sean F y f dos funciones aritméticas relacionadas por

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

Entonces

$$f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right)F(d).$$

Demostración: La igualdad de las sumas a la derecha se obtiene cambiando el índice de sumación d por $d' = \frac{n}{d}$.

Desarrollando los cálculos se tiene

$$\sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} f(c)\right) = \sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d)f(c)\right). \tag{7.1}$$

Resulta fácil comprobar que $d|n$ y $c|\frac{n}{d}$ si y sólo si $c|n$ y $d|\frac{n}{c}$. Así se tiene

$$\sum_{d|n} \left(\sum_{c|\frac{n}{d}} \mu(d)f(c)\right) = \sum_{c|n} \left(\sum_{d|\frac{n}{c}} f(c)\mu(d)\right) = \sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d)\right). \tag{7.2}$$

Pero ya se ha visto que la suma

$$\sum_{d|\frac{n}{c}} \mu(d)$$

se anula excepto cuando $\frac{n}{c} = 1$, es decir, cuando $n = c$, en cuyo caso vale 1. Entonces la parte derecha de (7.2) implica que

$$\sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) = \sum_{c=n} f(c) \cdot 1 = f(n),$$

de donde se deduce el teorema. **Q.e.d.**

A continuación se muestra para $n = 10$ el funcionamiento de la doble suma en (7.2). En este caso se tiene

$$\begin{aligned} \sum_{d|10} \left(\sum_{c|\frac{10}{d}} \mu(d) f(c) \right) &= \mu(1)[f(1) + f(2) + f(5) + f(10)] \\ &\quad +\mu(2)[f(1) + f(5)] + \mu(5)[f(1) + f(2)] + \mu(10) f(1) \\ &= f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] \\ &\quad +f(2)[\mu(1) + \mu(5)] + f(5)[\mu(1) + \mu(2)] + f(10)\mu(1) \\ &= \sum_{c|10} \left(f(c) \sum_{d|\frac{10}{c}} \mu(d) \right). \end{aligned}$$

Para estudiar la forma en que actúa la fórmula de inversión de Möbius, recordemos que las funciones τ y σ se expresan en la forma

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d.$$

La fórmula de inversión de Möbius indica que esas fórmulas pueden ser invertidas en la forma

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(n), \qquad n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(n)$$

para todo $n \geq 1$.

El teorema 7.1.2 garantiza que si f es una función multiplicativa, entonces la función $F(n) = \sum_{d|n} f(d)$ es también multiplicativa, pues $\sum_{d|n} f(d) = 1 * f(n)$. El siguiente teorema muestra la validez del recíproco.

TEOREMA 7.1.7

Si F es una función multiplicativa y

$$F(n) = \sum_{d|n} f(d),$$

entonces f también es una función multiplicativa.

Demostración: Sean m y n primos relativos positivos. Recordemos que todo divisor de mn se puede escribir como $d = d_1 d_2$ tal que $d_1|m$, $d_2|n$ y $(d_1, d_2) = 1$. Entonces al aplicar la fórmula de inversión es

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{d_1|m,\ d_2|n} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{d_1|m,\ d_2|n} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) = f(m) f(n), \end{aligned}$$

lo que demuestra el teorema. No sobra decir que en esta demostración es esencial el carácter multiplicativo de μ y de F. **Q.e.d.**

La función ϕ de Euler

Ya se ha definido $\phi(m)$ como la cantidad de números naturales primos relativos con m y menores que m. Como $1 * \phi(n) = n$ y que 1 y n son funciones multiplicativas, del teorema 7.1.7 se deduce que $\phi(n)$ es multiplicativa.

Por las fórmulas de Möbius es $\phi(n) = n * \mu(n)$. Entonces para $n = \prod_{i=1}^{r} p_i^{\nu_i}$ se cumple

$$\phi(n) = \prod_{i=1}^{r} \left(p_i^{\nu_i} - p_i^{\nu_i - 1}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

EJEMPLO: Calculemos $\phi(360)$. Como $360 = 2^3 3^2 5$, entonces

$$\begin{aligned} \phi(360) &= 360 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= 360 \left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 96. \end{aligned}$$

El lector atento notará que, excepto $\phi(1)$ y $\phi(2)$, los restantes valores de $\phi(n)$ parecen ser pares. Esto no es accidental, como muestra el siguiente teorema.

TEOREMA 7.1.8 *Para todo $n > 2$, $\phi(n)$ es un entero par.*

Demostración: Sea primero n una potencia de 2, es decir, $n = 2^k$ con $k \geq 2$. Se conoce que

$$\phi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$$

es un número par. Como, ϕ es multiplicativa, el teorema vale para todo entero n que sea divisible por una potencia de 2 de ese tipo.

Si n no contiene una potencia de 2 de ese tipo, entonces n tiene un factor primo p impar, es decir, $n = p^k m$ con $k \geq 1$ y $(p^k, m) = 1$. Entonces

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m)$$

es también un número par, por ser $p - 1$ par. **Q.e.d.**

Se puede demostrar ahora el Teorema de Euclides sobre la infinitud de los números de la siguiente manera: Como antes, asumimos que existe sólo una cantidad de números primos $p_1, p_2, \ldots, p_r$ y consideremos el número

$$n = p_1 p_2 \cdots p_r.$$

Si $1 < a \leq n$, entonces $(a, n) \leq 1$. En efecto, el Teorema Fundamental de la Aritmética asegura que a tiene un divisor primo q, que tiene que ser uno de los $p_1, p_2, \ldots, p_r$, por ser los únicos números primos. Entonces $q|n$, es decir, $(a, n) \geq q$. Todo ello implica que $\phi(n) = 1$, lo cual es imposible.

DEFINICIÓN 7.1.6 *La **función de Mangoldt** $\Lambda(n)$ se define por la relación*

$$1 * \Lambda(n) = \log n.$$

- La función de Mangoldt[3] $\Lambda(n)$ no es multiplicativa, $\Lambda(1) = 0$.
- Por las fórmulas de Möbius es

$$\Lambda(n) = \mu(n) * \log n = \sum_{t|n} \mu(t) \log\left(\frac{n}{t}\right) = -\sum_{t|n} \mu(t) \log t. \tag{7.3}$$

  Entonces para $n = p^\mu$ es

$$\Lambda(p^\nu) = \log p.$$

- Si $n = n_1 n_2$ con $1 < n_1 < n$ y $(n_1, n_2) = 1$, descomponiendo en (7.3) $t = t_1 t_2$ con $t_1|n_1$ y $t_2|n_2$, se obtiene

$$\Lambda(n_1 n_2) = \sum_{t_1|n_1} \sum_{t_2|n_2} \mu(t_1)\mu(t_2)(\log t_1 + \log t_2) = 0,$$

  pues $1 * \mu(n) = 0$ para $n > 1$.

[3] Hans Carl Friedrich Mangoldt (1851-1925)

7.2. Series de Dirichlet

DEFINICIÓN 7.2.1

Sea $f(n)$ una función aritmética. La serie

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

se conoce como ***serie de Dirichlet*** *de $f(n)$.*

Es conocido que si la serie $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge absoluto para $s = s_0$, entonces también converge absoluto para $s > s_0$. De aquí que a toda función aritmética $f(n)$ que tenga alguna serie de Dirichlet convergente, le corresponde una única función de variable real s

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

El siguiente teorema se refiere al recíproco.

TEOREMA 7.2.1

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = 0 \quad \forall\ s > s_0 \qquad \Rightarrow \qquad f(n) = 0.$$

Demostración: Supongamos que $f(n) = 0$ para $n < m$, pero $f(m) \neq 0$. Entonces para $s > s_0$ es

$$0 = \frac{f(m)}{m^s} + \sum_{n=m+1}^{\infty} \frac{f(n)}{n^s} = \frac{f(m)}{m^s} + \sum_{k=1}^{\infty} \frac{f(m+k)}{(m+k)^s} = \frac{f(m)}{m^s}(1 + G(s)), \tag{7.4}$$

con

$$G(s) = \sum_{k=1}^{\infty} \frac{f(m+k)}{m+k} \left(\frac{m}{m+k}\right)^s.$$

Si $s_0 < s_1 < s$, entonces

$$\left(\frac{m}{m+k}\right)^s = \left(\frac{m}{m+k}\right)^{s-s_1} \left(\frac{m}{m+k}\right)^{s_1} \leq \left(\frac{m}{m+1}\right)^{s-1} \left(\frac{m}{m+k}\right)^{s_1}.$$

Luego, se tiene

$$|G(s)| \leq \left(\frac{m}{m+k}\right)^{s-s_1} \frac{m^{s_1}}{f(m)} \sum_{k=1}^{\infty} \frac{|f(m+k)|}{(m+k)^{s_1}},$$

por lo que $G(s) \to 0$ cuando $s \to \infty$. Entonces en (7.4) se puede considerar a $|1 + G(s)| > \frac{1}{2}$ para s suficientemente grande, lo que contradice la suposición de que $f(m) \neq 0$ y (7.4). **Q.e.d.**

Las series de Dirichlet ofrecen una relación entre las funciones aritméticas y las de una variable real.

Sean las series absolutamente convergentes para $s > s_0$

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{y} \qquad G(s) = \sum_{m=1}^{\infty} \frac{g(m)}{m^s}.$$

Se conoce que toda serie, que recorre los productos $\frac{f(n)}{n^s}\frac{g(m)}{m^s}$ en cualquier orden, converge absoluto para $s > s_0$ a $F(s)G(s)$, es decir,

$$F(s)G(s) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{f(n)g(m)}{(nm)^s} = \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{nm=k} f(n)g(m).$$

Así, si se define

$$F(s)G(s) = H(s) = \sum_{k=1}^{\infty} \frac{h(k)}{k^s},$$

entonces

$$h(n) = f(n) * g(n).$$

Entonces la multiplicación de Dirichlet equivale a la multiplicación de series de Dirichlet.

Si hay convergencia, de la igualdad $H(s) = F(s)G(s)$ se puede deducir la de la función $h(n) = f(n) * g(n)$ y viceversa. De la solución de la ecuación aritmética en $f(n)$ se puede deducir fácilmente la de la ecuación $F(s) = \frac{H(s)}{G(s)}$ a través de la representación de $\frac{1}{G(s)}$ como serie de Dirichlet.

Teorema 7.2.2

Si $f(n)$ es una función multiplicativa y $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge absoluta para $s > s_0$, entonces para $s > s_0$ se cumple

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(\sum_{k=1}^{\infty} \frac{f(p^k)}{p^{ks}} \right).$$

Si $f(n)$ es totalmente multiplicativa, entonces

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

Demostración: Para p primo hacemos

$$F_p(s) = \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}} \qquad \text{para} \quad s > s_0.$$

Así

$$\prod_{p\le p_r} F_p(s) = \sum_{k_i=0}^{\infty} \cdots \sum_{k_r=0}^{\infty} \frac{f(p_1^{k_1})\cdots(p_r^{k_r})}{p_1^{k_1 s}\cdots p_r^{k_r s}}.$$

Como $f(n)$ es multiplicativa, se tiene

$$\prod_{p\le p_r} F_p(s) = \sum_{r} \frac{f(r)}{r^s},$$

donde la suma de la derecha se desarrolla sobre todos los $r \in \mathbb{N}$ que se forman por $p \le p_r$. Pero cuando $r \to \infty$ es

$$\left|\sum_{n=1}^{\infty} \frac{f(n)}{n^s} - \sum_{r} \frac{f(r)}{r^s}\right| \le \sum_{n=p_r+1}^{\infty} \frac{|f(n)|}{n^s} \to 0,$$

de donde

$$\sum_{r} \frac{f(r)}{r^s} \to \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{cuando} \quad r \to \infty.$$

El producto converge cuando la suma de los logaritmos converge y $\log(1+x) \le x$ para $x > -1$. Entonces

$$\begin{aligned}\left|\log \prod_{p\le p_r} F_p(s)\right| &\le \sum_{p\le p_r} |\log F_p(s)| = \sum_{p\le p_r} \left|\log\left(1 + \sum_{k=1}^{\infty} \frac{f(p^k)}{p^{ks}}\right)\right| \\ &\le \sum_{p\le p_r}\sum_{k=1}^{\infty} \frac{|f(p^{ks})|}{p^{ks}} \le \sum_{k=2}^{\infty} \frac{|f(n)|}{n^s}.\end{aligned}$$

De la acotación de las sumas parciales se deduce la convergencia de la serie y del producto. Entonces

$$\prod_{p} F_p(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

donde el producto se desarrolla sobre todos los números primos.

Si $f(n)$ es totalmente multiplicativa, entonces

$$F_p(s) = \frac{1}{1 - f(p)p^{-s}}.$$

Q.e.d.

La función zeta de Riemann[4] es una de las más nombradas de la Teoría de Números, no solo por su relación con las restantes funciones aritméticas, sino también por su protagonismo en una de las más famosas conjeturas de Matemática: la conjetura de Riemann, que es el más importante y único de los llamados problemas de siglo XX que se mantiene sin respuesta.

[4]Bernhard Riemann (1826-1866)

DEFINICIÓN 7.2.2 *La **función zeta de Riemann** se define como*

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

Por el teorema 7.2.2 es

$$\zeta(s) = \prod_{p} \frac{1}{1-p^{-s}}.$$

A continuación se presenta la relación de la función zeta de Riemann con las restantes funciones aritméticas aquí estudiadas.

La función de Möbius μ

Como $1 * \mu(n) = \epsilon(n)$ para $s > 1$, entonces

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

de donde

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

Las funciones de divisores

Para $s > \text{máx}(1, k+1)$ es

$$\zeta(s)\zeta(s-k) = \sum_{t=1}^{\infty} \frac{1}{t^s} \sum_{d=1}^{\infty} \frac{1}{d^{s-k}} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{td=n} d^k,$$

de donde

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

Números libres de cuadrados

Un número libre de cuadrados queda descrito por $|\mu(n)|$, pues

$$|\mu(n)| = \begin{cases} 1 & n \text{ libre de cuadrados} \\ 0 & \text{en otro caso} \end{cases}.$$

Como $\mu(n)$ es multiplicativa, aplicando el teorema 7.2.2 para $s > 1$ es

$$\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} = \prod_{p} (1 - p^{-s}) = \prod_{p} \frac{1-p^{-2s}}{1-p^{-s}},$$

de donde

$$\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} = \frac{\zeta(s)}{\zeta(2s)}.$$

La función ϕ de Euler

Como $\phi(n) = n * \mu(n)$, entonces para $s > 2$ es

$$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{td=n} t\mu(d) = \sum_{t=1}^{\infty} \frac{1}{t^{s-1}} \sum_{t=1}^{\infty} \frac{\mu(d)}{d^s},$$

de donde

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

Los factores primos de n

Para el número de diferentes factores primos de n se cumple

$$\omega(n_1 n_2) = \omega(n_1)\omega(n_2) \qquad \text{para} \qquad (n_1, n_2) = 1.$$

Entonces $2^{\omega(n)}$ es multiplicativa. Por el teorema 7.2.2 se tiene

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} &= \prod_p \left(\sum_{k=0}^{\infty} \frac{2^{\omega(p^k)}}{p^{ks}} \right) = \prod_p \left(1 + 2 \sum_{k=1}^{\infty} \frac{1}{p^{ks}} \right) \\ &= \prod_p \frac{1+p^{-s}}{1-p^{-s}} = \prod_p \frac{1+p^{-2s}}{(1-p^{-s})^2}, \end{aligned}$$

de donde

$$\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}.$$

La función $\Lambda(n)$ de Mangoldt

Recordemos que $\Lambda(n) = \log p$ para $n = p^\nu$ y $\Lambda(n) = 0$ en otro caso. Entonces para $s > 1$ es

$$\sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} \frac{1}{n^s} = \sum_p \sum_{k=1}^{\infty} \frac{1}{k} \frac{2^{\omega(p^k)}}{p^{ks}} = -\sum_p \log(1 - p^{-s}),$$

de donde

$$\sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} \frac{1}{n^s} = \log \zeta(s).$$

Esta expresión se puede derivar término a término, por lo que

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

7.3. El teorema de los números primos

Finalmente llegamos al punto en que se presenta el famoso teorema de los números primos que ya ha sido anunciado en el primer capítulo.

Definición 7.3.1

Para números reales positivos de define la función $\pi(x)$ como la ***cantidad de números primos menores o iguales a*** *x.*

De la demostración euclidiana de la infinitud de los números se dedujo que para el n-ésimo número primo p_n se cumple

$$p_n \leq 2^{2^{n-1}}.$$

Para $x \geq 2$ existe un entero $n \geq 0$ tal que

$$2^{2^n} \leq p_{n+1} < 2^{2^{n+1}}.$$

Entonces es

$$\pi(x) \geq \pi\left(2^{2^n}\right) \geq \pi(p_{n+1}) = n+1 > \frac{1}{\log 2}(\log\log x - \log\log 2),$$

de donde

$$\pi(x) > \frac{\log\log x}{\log 2}.$$

Para mejorar esa acotación usaremos la conocida fórmula del producto de Euler

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

Teorema 7.3.1

El producto $\prod_p \left(1 - \frac{1}{p}\right)^{-1}$ y la suma $\sum_p \frac{1}{p}$, tomados sobre todos los números primos p, son divergentes. En particular para $x \geq 2$ se cumple

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} > \log x \tag{7.5}$$

$$\sum_{p \leq x} \frac{1}{p} > \log\log x - 1. \tag{7.6}$$

Demostración: Al aplicar la fórmula del producto de Euler se tiene

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \leq x} \frac{1}{n},$$

donde la suma de la derecha se toma sobre todos los $n \in \mathbb{N}$ que se forman a partir de los primos $p \leq x$. Obviamente esa suma es convergente (por ser finita). Entonces

$$\begin{aligned}\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1} &\geq \sum_{n\leq x}\frac{1}{n}=\sum_{n\leq x}\int_n^{n+1}\frac{1}{n}dt\\ &\geq \int_1^{[x]+1}\frac{dt}{t}=\log([x]+1)>\log x,\end{aligned}$$

es decir

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}>\log x.$$

Hallando ahora logaritmo en la expresión anterior es

$$\begin{aligned}\log\log x &< -\prod_{p\leq x}\log\left(1-\frac{1}{p}\right)=\sum_{p\leq x}\sum_{n=1}^{\infty}\frac{1}{np^n}\\ &< \sum_{p\leq x}\sum_{n=1}^{\infty}\frac{1}{p^n}=\sum_{p\leq x}\frac{1}{p-1}\\ &= \sum_{p\leq x}\frac{1}{p}+\sum_{n=2}^{\infty}\left(\frac{1}{p-1}-\frac{1}{p}\right)<\sum_{p\leq x}\frac{1}{p}+\sum_{n=2}^{\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right)\\ &= \sum_{p\leq x}\frac{1}{p}+1,\end{aligned}$$

es decir

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

Q.e.d

De 7.5 se obtiene una mejora de la acotación por debajo de $\pi(x)$, pues

$$\log x<\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}=\prod_{n=1}^{\pi(x)}\left(1-\frac{1}{n+1}\right)^{-1}=\pi(x)+1,$$

es decir

$$\pi(x)>\log x-1.$$

Entonces para el n-ésimo número primo p_n es

$$n=\pi(n)>\log p_n-1,$$

de donde

$$p_n<e^{n+1}.$$

Utilizaremos ahora la criba de Erathostenes (algo modificada) para obtener una sencilla acotación por arriba de $\pi(x)$. En la lista de los n primeros números naturales tachamos todos los números primos y sus múltiplos bajo $\sqrt{x}$, por lo que quedan $1+\pi(x)-\pi(\sqrt{x})$ números sin tachar. Esos números sin tachar son primos relativos con todo $p \leq \sqrt{x}$, es decir, con $P = \prod_{p \leq \sqrt{x}} p$. Entonces

$$\begin{aligned} 1+\pi(x)-\pi(\sqrt{x}) &= -\sum_{np \leq x,\ (n,p)=1} 1 = \sum_{n \leq x} \sum_{t \mid np} \mu(t) \\ &= \sum_{t \mid p} \mu(t) \sum_{np \leq x,\ n \equiv 0 (mod\ t)} 1 = \sum_{t \mid p} \mu(t) \sum_{tm \leq x} 1, \end{aligned}$$

de donde

$$\pi(x) = \pi(\sqrt{x}) - 1 + \sum_{t \mid p} \mu(t) \left[\frac{x}{t} \right].$$

Sea ahora $P_y = \prod_{p \leq y} p$ con $y \leq \sqrt{x}$ y sea

$$N(x) = \sum_{n \leq x,\ (n,P_y)=1} 1 = \sum_{t \mid P_y} \mu(t) \left[\frac{x}{t} \right].$$

Obviamente es $N(x) \geq \pi(x) - \pi(y)$, por lo que para todo $y \leq \sqrt{x}$ se tiene

$$\pi(x) \leq \pi(y) + \sum_{t \mid P_y} \mu(t) \left[\frac{x}{t} \right].$$

Ahora seleccionamos y que optimice la acotación y se tiene

$$\begin{aligned} \pi(x) &\leq \pi(y) + \sum_{t \mid P_y} \mu(t) \frac{x}{t} + \sum_{t \mid P_y} 1 = \pi(y) + \frac{x}{P_y} \phi(P_y) + d(P_y) \\ &= \pi(y) + x \prod_{p \leq y} \left(1 - \frac{1}{p} \right) + 2^{\pi(y)} < y + \frac{x}{\log y} + 2^y \\ &< \frac{x}{\log y} + 2^{y+1}. \end{aligned}$$

Haciendo $y = \log x$ es

$$\pi(x) < \frac{x}{\log \log x} + 2^{\log x + 1},$$

de donde se obtiene para $x \geq e^3$

$$\pi(x) < \frac{2x}{\log \log x}.$$

Uno de los teorema más importantes de la Teoría de Números es el siguiente, que ofrecemos sin demostración.

TEOREMA 7.3.2 ***Teorema de los números primos***

Para la cantidad de números primos menores que un número real dado x se cumple

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1, \qquad \textit{es decir,} \qquad \pi(x) \sim \frac{x}{\pi(x)}.$$

Legendre[5] fue el primero en desarrollar una conjetura importante respecto a funciones que ofrezcan una buena aproximación de $\pi(x)$ para x grande. En su libro "Essai sur la Théorie des Nombres" (1798), Legendre conjeturó que $\pi(x)$ es aproximadamente igual a la función

$$\frac{x}{\log x - 1{,}08366}.$$

Calculando tablas de primos en 1000 enteros consecutivos, Gauss llegó a la conclusión de que $\pi(x)$ crece aproximadamente en el mismo orden que la función $\frac{x}{\log x}$ y con la integral logarítmica

$$Li(x) = \int_2^x \frac{du}{\log u}$$

obtiene una mejor aproximación numérica. Gauss comunicó sus observaciones al astrónomo Encke en 1849, y las publicó en 1863, pero parecen haber sido realizadas en 1791 cuando Gauss tenía 14 años (mucho antes que Legendre).

El primer progreso en la comparación de $\pi(x)$ con $\frac{x}{\log x}$ se debe al matemático ruso Tchebychef[6]. En 1850, demostró que existen constantes positivas a, b con $a < 1 < b$ tales que para x suficientemente grande se cumple

$$a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}.$$

Tchebychef mostró además que si el cociente $\frac{\pi(x)\log x}{x}$ converge cuando $x \to \infty$, entonces el límite tiene que ser 1. Pero Tchebychef no pudo demostrar la existencia del límite y pasaron 45 años hasta que ello logró demostrarse.

Las ideas radicalmente nuevas que dieron con la clave para demostrar el teorema de los números primos fueron introducidas por Riemann en su importante artículo "Über die Anzahl der Primzahlen unter einer gegebenen Grösse" de 1859 (su único artículo en la Teoría de Números). Mientras que Euler restringió la función $\zeta(s)$ a valores reales de s, Riemann reconoció la conexión entre la distribución de primos y el comportamiento de $\zeta(s)$ como función de la variable compleja $s = a + bi$. Enunció importantes propiedades de la función ζ, entre las que destaca una identidad, conocida como **fórmula explícita de Riemann**, que relaciona a $\pi(x)$ con los ceros de la

[5] Adrien Marie Legendre (1752-1833)
[6] Pafnuty Lvovich Tchebychef (1821-1894)

función $\zeta(s)$ en el plano complejo. El resultado cautivó la imaginación de muchos matemáticos por lo inesperado de la relación de procesos de la Teoría de Números (que son discretos) con el Análisis Complejo (que trata de procesos continuos). En su memoria, Riemann desarrolló importantes conjeturas relacionadas con los ceros de la función $\zeta(s)$. El más famoso, conocido como **conjetura de Riemann**, afirma que todos los ceros no reales de la función $\zeta(s)$ se encuentran sobre la recta $Re(s) = \frac{1}{2}$ y aún no ha podido ser demostrado.

Las investigaciones de Riemann dieron pié a los trabajos de Hadamard[7] y de la Vallee Poussin[8], quienes (simultánea e independientemente) demostraron en 1896 el teorema de los números primos.

Hasta mediados del siglo pasado prevalecía la idea de que el teorema de los números primos no podía ser demostrado sin utilizar las propiedades de la función ζ de Riemann y sin los recursos de la teoría funciones de variable compleja. Por ello resultó una gran sorpresa cuando el matemático noruego Atle Selberg[9] encontró en 1949 una demostración puramente aritmética. Su artículo "An Elementary Proof of the Prime Number Theorem" es "elemental" en el sentido de que evita los métodos del análisis moderno, pero es en extremo complicada. Se cuenta que en la misma época el matemático húngaro Paul Erdös[10] logró también demostrar con métodos "elementales" el teorema y que lo comentó con Selberg, el cual no le dió crédito en su artículo. Selberg recibió por su trabajo en esta área la medalla Fields en el Congreso de Matemáticos de 1950.

7.4. Ejercicios del capítulo

1. Sean m y n enteros positivos y sean $p_1, p_2, \ldots, p_r$ primos diferentes que dividen al menos uno de m o n. Entonces m y n pueden ser escritos en la forma

$$\begin{aligned} m &= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad \text{con} \quad k_i \geq 0 \quad \text{para } i = 1, 2, \ldots, r \\ n &= p_1^{j_1} p_2^{j_2} \cdots p_r^{j_s} \quad \text{con} \quad j_i \geq 0 \quad \text{para } i = 1, 2, \ldots, r. \end{aligned}$$

   Demuestre que

$$(m, n) = p_1^{u_1} p_2^{u_2} \cdots p_r^{u_s}, \qquad [m, n] = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_s},$$

   donde $u_i = \text{mín}\{k_i, j_i\}$ y $v_i = \text{máx}\{k_i, j_i\}$.

2. Use el problema 1 para calcular $(12378, 3054)$ y $[12378, 3054]$.

[7] Jacques Hadamard (1865-1963)
[8] Charles de la Vallee Poussin (1866-1962)
[9] Atle Selberg (1917-2007)
[10] Paul Erdös (1913-199)

3. Deduzca del problema 1 que $(m,n)[m,n] = mn$ para enteros positivos m y n.

4. En la notación del problema 1, muestre que $(m,n) = 1$ si y sólo si $k_i j_i = 0$ para $i = 1, 2, \ldots, r$.

5. *a*) Compruebe que para $n = 3655$ y 4503 se cumple

$$\tau(n) = \tau(n+1) = \tau(n+2) = \tau(n+3).$$

   b) Si $n = 14,206$ y 957, muestre que $\sigma(n) = \sigma(n+1)$.

6. Para todo entero $n \geq 1$, establezca la desigualdad $\tau(n) < s\sqrt{n}$. (Sugerencia: si $d|n$, entonces uno de d o $\frac{n}{d}$ es menor o igual a $\sqrt{n}$.)

7. Demuestre que:

   a) $\tau(n)$ es un entero impar si y sólo si n es un cuadrado perfecto.

   b) $\sigma(n)$ es un entero impar si y sólo si n es un cuadrado perfecto o el doble de un cuadrado perfecto. (Sugerencia: si p es un primo impar, entonces $1 + p + p^2 + \ldots + p^k$ es impar sólo cuando k es par.)

8. Demuestre que para todo entero positivo n se cumple

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

9. Si n es un entero libre de cuadrados, demuestre que $\tau(n) = 2^r$, donde r es el número de divisores primos de n.

10. Demuestre las siguientes proposiciones:

   a) Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ es la factorización prima de $n > 1$, entonces

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

   b) Para todo entero positivo n se cumple

$$\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.$$

   (Sugerencia: ver problema 8.)

   c) Si $n > 1$ es un entero compuesto, entonces $\sigma(n) > n + \sqrt{n}$. (Sugerencia: Sea $d|n$, donde $1 < d < n$, entonces $1 < \frac{n}{d} < n$, si $d \leq \sqrt{n}$, entonces $\frac{n}{d} \geq \sqrt{n}$.)

11. Dado un entero $k > 1$, muestre que existen infinitos enteros n, para los cuales $\tau(n) = k$, pero a lo sumo hay una cantidad finita de n con $\sigma(n) = k$. (Sugerencia: utilice el problema 10a).

12. *a*) Halle la forma de todos los enteros n que cumplen $\tau(n) = 10$. ¿cuál es el menor entero positivo para el que esto es cierto?

    b) Demuestre que no hay enteros positivos n para los que $\sigma(n) = 10$. (Sugerencia: note que para $n > 1$ se tiene $\sigma(n) > n$.)

13. Demuestre que hay infinitos pares de enteros m y n con $\sigma(m^2) = \sigma(n^2)$. (Sugerencia: seleccione k tal que $(k, 10) = 1$ y considere los enteros $m = 5k$, $n = 4k$.)

14. Para $k \geq 2$ demuestre:

    a) $n = 2^{k-l}$ cumple $\sigma(n) = 2n - 1$.

    b) Si $2^k - 1$ es primo, entonces $n = 2^{k-1}(2^k - 1)$ cumple $\sigma(n) = 2n$.

    c) Si $2^k - 3$ es primo, entonces $n = 2^{k-1}(2^k - 3)$ cumple $\sigma(n) = 2n - 2$.

    No se conoce si hay enteros n, para los cuales $\sigma(n) = 2n + 1$.

15. Si n y $n + 2$ son primos gemelos, compruebe que $\sigma(n + 2) = \sigma(n) + 2$, esto también se cumple para $n = 434$ y 8575.

16. *a*) Para todo entero $n > 1$, Demuestre que existen enteros n_1 y n_2 con $\tau(n_1) + \tau(n_2) = n$.

    b) Demuestre que la conjetura de Goldbach implica que para todo entero par $2n$ existen enteros n_1 y n_2 con $\sigma(n_1) + \sigma(n_2) = 2n$.

17. Para un entero fijo k, demuestre que la función f definida por $f(n) = n^k$ es multiplicativa.

18. Sean f y g funciones multiplicativas tales que $f(p^k) = g(p^k)$ para todo primo p y $k \geq 1$. Demuestre que $f = g$.

19. Demuestre que si f y g son funciones multiplicativas, entonces también lo es su producto fg y su cociente $\frac{f}{g}$ (siempre que esté definido).

20. Se define la función ρ por $\rho(1) = 1$ y $\rho(n) = 2^r$, si la factorización prima de $n > 1$ es $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Por ejemplo, $\rho(8) = 2$ y $\rho(10) = \rho(36) = 2^2$.

    a) Demuestre que ρ es una función multiplicativa.

    b) Halle una fórmula para
    $$F(n) = \sum_{d|n} \rho(d)$$
    en términos de la factorización prima de n.

21. Para todo entero positivo n, demuestre que

$$\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d) \right)^2 .$$

(Sugerencia: ambos miembros de la ecuación son funciones multiplicativas de n, de modo que basta considerar el caso $n = p^k$, donde p es primo.)

22. Dado $n > 0$, sea $\sigma_s(n)$ la suma de las potencias de orden s de los divisores positivos de n, es decir,

$$\sigma_s(n) = \sum_{d|n} d^s.$$

Compruebe que:

a) $\sigma_0 = \tau$ y $\sigma_1 = \sigma$.

b) σ_s es una función multiplicativa. (Sugerencia: la función f, definida por $f(n) = n^s$ es multiplicativa.)

c) Si $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ es la factorización prima de n, entonces

$$\sigma_s(n) = \left(\frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1} \right) \left(\frac{p_2^{s(k_2+1)} - 1}{p_2^s - 1} \right) \cdots \left(\frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1} \right).$$

23. Para todo entero postivo n, demuestre que

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

b) $\sum_{d|n} \frac{n}{d} \sigma(d) = \sum_{d|n} d\tau(d)$. (Sugerencia: como las funciones $F(n) = \sum_{d|n} \sigma(d)$ y $G(n) = \sum_{d|n} \frac{n}{d} \tau(d)$ son multiplicativas, basta demostrar que $F(p^k) = G(p^k)$ para todo primo p.)

24. *a)* Para todo entero positivo n, demuestre que

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$

b) Para todo entero positivo $n \geq 3$, demuestre que

$$\sum_{k=1}^{n} \mu(k!) = 1$$

.

25. La función de Mangoldt Λ está definida como

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^k, \text{ con } p \text{ primo y } k \geq 1 \\ o & \text{en otro caso} \end{cases}.$$

Demuestre que

$$\Lambda(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log d = -\sum_{d|n} \mu(d) \log d.$$

(Sugerencia: compruebe que

$$\sum_{d|n} \Lambda(d) = \log n$$

y aplique la fórmula de inversión de Möbius.)

26. Sea $n = p_l^{k_1} p_2^{k_2} \dots p_r^{k_r}$ la factorización prima de n. Si f es una función multiplicativa, demuestre que

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_l))(1 - f(p_2)) \cdots (1 - f(p_r)).$$

(Sugerencia: La función F, definida por

$$F(n) = \sum_{d|n} f(d)$$

es multiplicativa, entonces $F(n)$ es el producto de los valores de $F\left(p_i^{k1}\right)$.)

27. Si el entero $n > 1$ tiene la factorización prima $n = p_l^{k_1} p_2^{k_2} \dots p_r^{k_r}$, use el problema 3 para comprobar lo siguiente:

a) $\sum_{d|n} \mu(d)\tau(d) = (-1)^r$.

b) $\sum_{d|n} \mu(d)\sigma(d) = (-1)^r p_l p_2 \cdots p_r$.

c) $\sum_{d|n} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.

d) $\sum_{d|n} d\mu(d) = (1 - p_1)(1 - p_2) \cdots (1 - p_r)$.

28. Sea $S(n)$ el número de divisores de n libres de cuadrado. Compruebe que

$$S(n) = \sum_{d|n} |\mu(d)| = 2^r,$$

donde r es el número de divisores primos diferentes de n. (Sugerencia: S es una función multiplicativa.)

29. Encuentre fórmulas para

$$\sum_{d|n} \frac{\mu^2(d)}{\tau(d)} \quad \text{y} \quad \sum_{d|n} \frac{\mu^2(d)}{\sigma(d)}$$

en términos de la factorización prima de n.

30. La λ-**función de Liouville** está definida por $\lambda(1) = 1$ y $\lambda(n) = (-1)^{k_1+\ldots+k_r}$ si la factorización prima de $n > 1$ es $n = p_l^{k_1} p_2^{k_2} \ldots p_r^{k_r}$

a) Demuestre que λ es una función multiplicativa.

b) Dado un entero positivo n, compruebe que

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{si } n = m^2, \text{ para cierto entero } m \\ 0 & \text{en otro caso} \end{cases}.$$

31. Si el entero $n > 1$ tiene la factorización prima $n = p_l^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, compruebe que

$$\sum_{d|n} \mu(d)\lambda(d) = 2^r.$$

32. Calcule $\phi(1001)$, $\phi(5040)$, y $\phi(36\ 000)$.

33. Compruebe para $n = 5186$ la igualdad $\phi(n) = \phi(n+1) = \phi(n+2)$.

34. Demuestre que los enteros $m = 3^k 568$ y $n = 3^k 638$, donde $k \geq 0$, satisfacen simultáneamente

$$\tau(m) = \tau(n), \qquad \sigma(m) = \sigma(n), \qquad \phi(m) = \phi(n).$$

35. Demuestre las siguientes proposiciones:

a) Si n es un entero impar, entonces $\phi(2n) = \phi(n)$.

b) Si n es un entero impar, entonces $\phi(2n) = 2\phi(n)$.

c) $\phi(3n) = 3\phi(n)$ si y sólo si $3|n$.

d) $\phi(3n) = 2\phi(n)$ si y sólo si $3 \nmid n$.

e) $\phi(n) = \frac{n}{2}$ si y sólo si $n = 2^k$ para cierto $k > 1$. (Sugerencia: escriba $n = 2^k N$, con N impar, y use la condición $\phi(n) = \frac{n}{2}$ para comprobar que $N = 1$.)

36. Demuestre que la ecuación $\phi(n) = \phi(n+2)$ se cumple para $n = 2(2p-1)$ siempre que p y $2p-1$ sean ambos primos impares.

37. Demuestre que existen infinitos enteros n para los cuales $\phi(n)$ es un cuadrado perfecto (Sugerencia: considere los enteros $n = 2^k + l$ para $k = 1, 2, \ldots$)

38. Compruebe lo siguiente:

    a) Para todo entero positivo n es $\frac{1}{2}\sqrt{n} \leq \phi(n) < n$. (Sugerencia: escriba la factorización $n = 2^{k_0}p_1^{k_1}\cdots p_r^{k_r}$, de modo que

    $$\phi(n) = 2^{k_0-1}p_1^{k_1-1}\cdots p_r^{k_r-1}(p_1-1)\cdots(p_r-1);$$

    use las desigualdades $p-1 > \sqrt{p}$ y $k - \frac{1}{2} \geq \frac{k}{2}$ para obtener el valor $\phi(n) = 2^{k_0-1}p_1^{k_1/2}\cdots p_r^{k_r/2}$.)

    b) Si el entero $n > 1$ tiene r factores primos diferentes, entonces $\phi(n) \geq \frac{2}{n^r}$.

    c) Si $n > 1$ es compuesto, entonces $\phi(n) \leq n - \sqrt{n}$. (Sugerencia: sea p el menor divisor primo de n, de modo que $p \leq \sqrt{n}$, entonces se cumple $\phi(n) \leq n\left(1 - \frac{1}{p}\right)$.)

39. Demuestre que si n tiene factores primos impares diferentes, entonces $2^r|\phi(n)$.

40. Demuestre que:

    a) Si n y $n+2$ son primos gemelos, entonces $\phi(n2) = \phi(n)+2$; esto es válido también para $n = 12, 14$ y 20.

    b) Si p y $2p+1$ son primos impares, entonces $n = 4p$ satisface la relación $\phi(n+2) = \phi(n)+2$.

41. Si todo divisor primo de n divide también a m, demuestre que $\phi(nm) = n\phi(m)$. En particular, $\phi(n^2) = n\phi(n)$ para todo entero positivo n.

42. *a)* Si $\phi(n)|n-1$, demuestre que n es libre de cuadrados. (Sugerencia: asuma que n tiene la factorización prima $n = p_l^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, donde $k_i \geq 2$, entonces $p_1|\phi(n)$, de donde $p_1|(n-1)$, lo que conduce a una contradicción.)

    b) Demuestre que si $n = 2^k$ ó 2^k3^j con k y j enteros positivos, entonces $\phi(n)|n$.

43. Si $n = p_1^{k_1}\cdots p_r^{k_r}$ derive las desigualdades

    $$a) \qquad \sigma(n)\phi(n) \geq n^2\left(1-\frac{1}{p_1^2}\right)\cdots\left(1-\frac{1}{p_r^2}\right),$$
    $$b) \qquad \tau(n)\phi(n) \geq n$$

    (Sugerencia: compruebe que $\tau(n)\phi(n) \geq 2^r n\left(\frac{1}{2}\right)^r$.)

44. Demuestre que si $d|n$, entonces $\phi(d)|\phi(n)$. (Sugerencia: trabaje con las factorizaciones primas de d y n.)

45. Obtenga las siguientes generalizaciones del teorema que establece relaciones para la función de Euler:

a) Para enteros positivos m y n se cumple

$$\phi(m)\phi(n) = \frac{\phi(mn)\phi(d)}{d},$$

donde $d = (m, n)$.

b) Para enteros positivos m y n se cumple

$$\phi(m)\phi(n) = \phi((m, n))\phi([m, n]).$$

46. Demuestre que la conjetura de Goldbach implica que para todo entero par $2n$ existen enteros n_1 y n_2, con $\phi(n_1) + \phi(n_2) = 2n$.

47. Dado un entero positivo k, demuestre que

a) Existe a lo sumo una cantidad finita de enteros n tales que $\phi(n) = k$.

b) Si al ecuación $\phi(n) = k$ tiene solución única $n = n_0$, entonces $4|n_0$. (Sugerencia: ver problemas 4a) y 4b).)

Una famosa conjetura de Carmichael es que el número de soluciones de $\phi(n) = k$ no puede ser 1.

48. Halle todas las soluciones de $\phi(n) = 16$ y $\phi(n) = 24$. (Sugerencia: si el número $n = p_1^{k_1} \cdots p_r^{k_r}$ satisface $\phi(n) = k$, entonces

$$n = \left[\frac{k}{\prod(p_i - 1)}\right] \prod p_i;$$

así los enteros $d_i = p_i - 1$ pueden ser determinados por las condiciones (1) $d_i|k$, (2) $d_i + 1$ es primo y (3) $\frac{k}{\prod(p_i-1)}$ no contiene factor primo en $\prod p_i$.)

49. *a*) Demuestre que la ecuación $\phi(n) = 2p$ no tiene solución para p primo y $2p + 1$ compuesto.

b) Demuestre que no existe solución de la ecuación $\phi(n) = 14$, y que 14 es el menor entero (positivo) par con esta propiedad.

50. Si p es primo y $k \geq 2$, demuestre que $\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2)$.

51. Use el Teorema de Euler para demostrar:

a) $a^{37} = a(mod\ 1729)$ para todo entero a. (Sugerencia: $1729 = 7 \cdot 13 \cdot 19$.)

b) $a^{13} = a(mod\ 2730)$ para todo entero a. (Sugerencia: $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.)

c) $a^{33} = a(mod\ 4080)$ para todo entero a. (Sugerencia: $4080 = 15 \cdot 16 \cdot 17$.)

52. Demuestre que si $(a, n) = (a - 1, n) = 1$, entonces

$$1 + a + a^2 + \ldots + a^{\phi(n)-1} \equiv 0(mod\ n).$$

(Sugerencia: recuerde que $a^{\phi(n)} - 1 = (a - 1)(a^{\phi(n)-1} + ... + a^2 + a + 1)$.)

53. Si m y n son primos relativos, demuestre que

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1(mod\ mn).$$

54. Complete los detalles faltantes en la siguiente demostración del Teorema de Euler: Sea p un divisor primo de n y $(a, p) = 1$. Por el Teorema de Fermat es $a^{p-1} \equiv 1(mod\ p)$, de modo que $a^{p-1} = 1 + tp$ para cierto t. Entonces

$$a^{p(p-1)} = (1 + tp)^p = 1 + \binom{p}{1}(tp) + -.. + (tp)^p \equiv 1(mod\ p^2)$$

y, por inducción es $a^{p^{k-1}(p-1)} \equiv 1(mod\ p^k)$ con $k = 1, 2, \ldots$. Elevando ambos miembros de esta congruencia a la potencia $\phi(n)/p^{k-1}(p - 1)$ se obtiene la equivalencia $a^{\phi(n)} \equiv 1(mod\ p^k)$. Entonces $a^{\phi(n)} \equiv 1(mod\ n)$.

55. Halle el dígito de las unidades de 3^{100} aplicando el Teorema de Euler.

56. *a*) Si $(a, n) = 1$ muestre que la congruencia lineal $ax \equiv b(mod\ n)$ tiene la solución $x \equiv ba^{\phi(n)-1}(mod\ n)$.

    b) Use el inciso a) para solucionar las congruencias

$$3x \equiv 4(mod\ 26), \qquad 13x \equiv 2(mod\ 40), \qquad 10x \equiv 21(mod\ 49).$$

57. Demuestre que todo primo diferente de 2 y 5 divide a infinitos de los enteros $1, 11, 111, 1111, \ldots$.

58. Dado $n \geq 1$, un conjunto de $\phi(n)$ enteros incongruentes módulo n y primos relativos con n se llama *sistema reducido de restos módulo n* (es decir, un sistema reducido de restos módulo n lo conforman aquellos de un sistema completo de restos módulo n que son primos relativos con n). Demuestre que

    a) los enteros $-31, -16, -8, 13, 25, 80$ forman un sistema reducido de restos módulo 9;

    b) los enteros $3, 3^2, 3^3, 3^4, 3^5, 3^6$ forman un sistema reducido de restos módulo 14;

    c) los enteros $2, 2^2, 2^3, \ldots, 2^{18}$ forman un sistema reducido de restos módulo 27.

59. Si p es primo impar, muestre que los enteros

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2 \ldots, \frac{p-1}{2}$$

forman un sistema reducido de restos módulo p.

60. Para un entero positivo n, demuestre que

$$\sum_{d|n}(-1)^{\frac{n}{d}}\phi(d) = \begin{cases} 0 & \text{si } n \text{ es par} \\ -n & \text{si } n \text{ es impar} \end{cases}.$$

(Sugerencia: Si $n = 2^k N$ con N impar, entonces

$$\sum_{d|n}(-1)^{\frac{n}{d}}\phi(d) = \sum_{d|2^{k-1}N}(-1)^{\frac{n}{d}}\phi(d) - \sum_{d|N}(-1)^{\frac{n}{d}}\phi(2^k d) \quad .)$$

61. Compruebe que

$$\sum_{d|36}\phi(d) = 36 \quad \text{y} \quad \sum_{d|36}(-1)^{\frac{36}{d}}\phi(d) = 0.$$

62. Para un entero positivo n, demuestre que

$$\sum_{d|n}\frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}.$$

(Sugerencia: ver la sugerencia del problema 1.)

63. Use el problema 3 de la sección 6.2 para dar una demostración diferente de

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

64. Si el entero $n > 1$ tiene la factorización prima

$$n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r},$$

demuestre lo siguiente:

a) $$\sum_{d|n}\mu(d)\phi(d) = (2-p_1)(2-p_2)\cdots(2-p_r).$$

b) $$\sum_{d|n}d\phi(d) = \left(\frac{p_1^{2k_1+1}+1}{p_1+1}\right)\left(\frac{p_2^{2k_2+1}+1}{p_2+1}\right)\cdots\left(\frac{p_r^{2k_r+1}+1}{p_r+1}\right).$$

c) $$\sum_{d|n}\frac{\phi(d)}{d} = \left(1+\frac{k_1(p_1-1)}{p_1}\right)\left(1+\frac{k_2(p_2-1)}{p_2}\right)\cdots\left(1+\frac{k_r(p_r-1)}{p_r}\right).$$

(Sugerencia: Para a), use el problema 3 de la sección 6.2.)

65. Compruebe la fórmula

$$\sum_{d=1}^{n} \phi(d) \left[\frac{n}{d}\right] = \frac{n(n+1)}{2}$$

para todo entero positivo n. (Sugerencia: esto es una aplicación directa del teorema 1 de la sección 6.1 y del teorema **??**.)

66. Si n es un entero libre de cuadrados, demuestre que

$$\sum_{d|n} \sigma(d^{k-1})\phi(d) = n^k$$

para todo entero $k \geq 2$.

67. Para un un entero libre de cuadrados $n > 1$, demuestre que $\tau(n^2) = n$ si y sólo si $n = 3$.

68. Demuestre que $3|\sigma(3n+2)$ y $4|\sigma(4n+3)$ para todo entero positivo n.

69. *a*) Dado $k > 0$, demuestre que existe una sucesión de k enteros consecutivos $n+1, n+2, \ldots, n+k$ tales que $\mu(n+l) = \mu(n+2) = \ldots = \mu(n+k) = 0$. (Sugerencia: Considere el sitema de congruencias lineales

$$\begin{aligned} x &\equiv -1 (mod\ 4) \\ x &\equiv -2 (mod\ 9) \\ \ldots &\quad \ldots \\ x &\equiv -k (mod\ p_k^2) \end{aligned}$$

´donde p_k es el k-ésimo primo.)

b) Halle cuatro enteros consecutivos para los cuales $\mu(n) = 0$.

70. Demuestre las siguientes proposiciones:

a) Un entero n es primo si y sólo si $\sigma(n) + \phi(n) = n\tau(n)$. (Sugerencia: derive primero la relación

$$\sum_{d|n} \sigma(d)\phi\left(\frac{n}{d}\right) = n\tau(n) \quad .)$$

b) Un entero n es primo si y sólo si $\phi(n)|n-1$ y $n+1|\sigma(n)$. (Sugerencia: ver problema lla) de la sección 7.2.)

71. Demuestre que existen infinitos enteros n tales que $\phi(n) = \frac{n}{3}$, y para ninguno de los cuales es $\phi(n) = \frac{n}{4}$.

72. Para $n > 2$, demuestre la desigualdad $\phi(n^2) + \phi((n+1)^2 \leq 2n^2$.

Capítulo 8

NÚMEROS INTERESANTES

8.1. Números perfectos

En la historia de la Teoría de Números abundan las conjeturas famosas y los problemas abiertos. Este epígrafe trata de ciertas intrigantes conjeturas asociadas a los números perfectos. Algunas de ellas ya han sido resueltas satisfactoriamente, pero la mayoría permanece sin resolver. Todas han estimulado el desarrollo del tema como un todo. Los pitagóricos consideraban notable que el número 6 es igual a la suma de sus divisores positivos propios:

$$6 = 1 + 2 + 3.$$

El siguiente número con esta propiedad es 28, pues

$$28 = 1 + 2 + 4 + 7 + 14.$$

De acuerdo a su filosofía de atribuir propiedades místicas a los números, los pitagóricos llamaron "perfectos" a esos números.

DEFINICIÓN 8.1.1

Un entero positivo n se dice ***perfecto*** *si n es igual a la suma de todos sus divisores positivos propios (es decir, diferentes de n mismo).*

La suma de los divisores positivos de un entero n, cada uno de los cuales es menor que n, está dada por $\sigma(n) - n$. Luego, la condición "n es perfecto" equivale a comprobar que $\sigma(n) - n = n$, o lo que es lo mismo

$$\sigma(n) = 2n.$$

Por ejemplo,

$$\begin{aligned} \sigma(6) &= 1 + 2 + 3 + 6 = 12 = 2 \cdot 6 \\ \sigma(28) &= 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28, \end{aligned}$$

por lo que 6 y 28 son números perfectos.

Durante muchos siglos, los filósofos estudiaron el significado místico o religioso de los números perfectos, más que sus propiedades matemáticas. Saint Augustine explica que Dios no pudo haber creado el mundo de una vez. El prefirió tomar 6 días, porque la perfección del trabajo queda simbolizada por el número (perfecto) 6. Comentaristas del Antiguo Testamento argumentaban que la perfección del Universo está representada por 28, el número de días que demora la luna en rotar alrededor de la Tierra. En la misma línea, el teólogo Almin of Yorkdel siglo VIII observó que toda la raza humana desciende de las ocho almas del Arca de Noé y esta segunda creación es menos perfecta que la primera, pues 8 es un número imperfecto.

Los griegos antiguos sólo conocieron cuatro números perfectos. Nicomachus[1] presenta la lista en su "Introductio Arithmeticae" (aprox. 100 A.C.)

$$P_1 = 6, \quad P_2 = 28, \quad P_3 = 496, \quad P_4 = 8128.$$

Comenta que están formados de una manera "ordenada", uno entre las unidades, uno entre las decenas, uno entre las centenas y uno entre los millares (es, decir, menor que 10 000). Basado en esa corta evidencia, conjeturó que:

(1) El n-ésimo número perfecto P_n contiene exactamente n dígitos;

(2) Los números perfectos pares terminan alternadamente en 6 y 8.

Ambas afirmaciones son erróneas. No existe ningún número perfecto con 5 dígitos; el siguiente número perfecto (aparecido en un manuscrito anónimo del siglo XV) es

$$P_5 = 33\ 550\ 336.$$

Mientras que el dígito final de P_5 es 6, el siguiente número perfecto

$$P_6 = 8\ 589\ 869\ 056$$

también termina en 6, y no en 8 como indicaría la conjetura. Salvando algo en la dirección positiva, veremos más adelante que todo número perfecto para termina en 6 u 8, pero no necesariamente en orden alterno.

Sólo la magnitud de P_6 ya podría convencer al lector de la rareza de los números perfectos. Aún no se conoce si existen finitos o infinitos de esos números.

El problema de determinar la forma general de los números perfectos data casi de los inicios de la era matemática. Fue parcialmente resuelto por Euclides, cuando en el libro IX de "Elementos" demostró que si la suma

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

[1]Nicomachus (ca. 100)

es un número primo, entonces $2^{k-1}p$ es un número perfecto (necesariamente par). Por ejemplo, $1+2+4=7$ es primo, por lo que $4 \cdot 7 = 28$ es un número perfecto. La demostración de Euclides usa la fórmula de la suma de la progresión geométrica

$$1 + 2 + 2^2 + \ldots + 2^{k-1} = 2^k - 1,$$

que se encuentra en varios textos pitagóricos. En esta notación, el resultado queda como sigue: Si $2^k - 1$ es primo ($k > 1$), entonces $n = 2^{k-1}(2^k - 1)$ es un número perfecto. Más de 2000 años después de Euclides, Euler dio un paso decisivo al demostrar que todos los números perfectos pares tienen que ser de esa forma. Ambas proposiciones aparecen en el siguiente teorema.

Teorema 8.1.1

Si $2^k - 1$ es primo ($k > 1$), entonces $n = 2^{k-1}(2^k - 1)$ es perfecto y todo número perfecto par es de esa forma.

Demostración: Sea $2^k - 1 = p$ primo y consideremos $n = 2^{k-1}p$. Como $(2^{k-1}, p) = 1$, la multiplicatividad de σ implica que

$$\begin{aligned} \sigma(n) &= \sigma\left(2^{k-1}p\right) = \sigma\left(2^{k-1}\right)\sigma(p) \\ &= (2^k - 1)(p+1) \\ &= (2^k - 1)2^k = 2n, \end{aligned}$$

por lo que n es un número perfecto.

Para el recíproco, asumimos que n es un número perfecto par. Podemos escribir $n = 2^{k-1}m$, donde m es un entero impar y $k \geq 2$. Como $(2^{k-1}, m) = 1$, se tiene que

$$\sigma(n) = \sigma\left(2^{k-1}m\right) = \sigma\left(2^{k-1}\right)\sigma(m) = (2^k - 1)\sigma(m),$$

mientras que la condición para que un número sea perfecto exige que

$$\sigma(n) = 2n = 2^k m.$$

Uniendo ambas relaciones es

$$2^k m = (2^k - 1)\sigma(m),$$

de donde se deduce que $(2^k - 1) | 2^k m$. Pero $2^k - 1$ y 2^k son primos relativos, por lo que $(2^k - 1) | m$, es decir, $m = (2^k - 1)M$. Ahora, al sustituir en la última ecuación se tiene $\sigma(m) = 2^k M$. Como m y M son divisores de m ($M < m$), es

$$2^k M = \sigma(m) \geq m + M = 2^k M,$$

por lo que $\sigma(m) = m + M$. De aquí que m sólo tiene dos divisores positivos, M y el mismo m, por lo que m tiene que ser primo y $M = 1$. En otras palabras,

$m = (2^k - 1)M = 2^k - 1$ es primo, lo que completa la demostración. **Q.e.d.**

Como el problema de buscar números perfectos pares se reduce a la búsqueda de los números primos de la forma $2^n - 1$, sería fructífera una mirada más cercana a esos enteros.

LEMA 8.1.1

Si $a^k - 1$ es primo ($a > 0, k \geq 2$), entonces $a = 2$ y k también es primo.

Demostración: Se puede comprobar fácilmente que

$$a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \ldots + a^2 + a + 1),$$

donde

$$a^{k-1} + a^{k-2} + \ldots + a^2 + a + 1 \geq a + 1 > 1.$$

Como $a^k - 1$ es primo, el otro factor tiene que se 1, es decir, $a - 1 = 1$, de donde $a = 2$.

Si k fuera compuesto, podríamos escribir $k = rs$ con $1 < r$ y $1 < s$. Entonces

$$a^k - 1 = (a^r)^s - 1 = (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + \ldots + a^r + 1),$$

y cada factor del miembro derecho es estrictamente mayor que 1. Pero ello viola la primalidad de $a^k - 1$, por lo que k tiene que ser primo. **Q.e.d.**

Para $p = 2, 3, 5, 7$, los valores $3, 7, 31, 127$ de $2^p - 1$ son primos, por lo que

$$\begin{aligned} 2(2^2 - 1) &= 6 \\ 2^2(2^3 - 1) &= 28 \\ 2^4(2^5 - 1) &= 496 \\ 2^6(2^7 - 1) &= 8128 \end{aligned}$$

son números perfectos.

Algunos antiguos autores creían erróneamente que $2^p - 1$ es primo para cualquier selección del número primo p. Pero en 1536, Hudalrichus Regius presentó en un trabajo llamado "Utriusque Arithmeth" la factorización correcta

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

Si ello pareciera poco mérito, nótese que los cálculos tuvieron que realizarse en números romanos con la ayuda de un ábaco (no fue hasta el siglo XVI que la numeración arabica ganó total ascendencia sobre la romana). Regius también dio a

$p = 13$ como el siguiente valor de p para el que el número $2^p - 1$ es primo. A partir de ello se obtiene el quinto número perfecto

$$2^{12}(2^{13} - 1) = 33\ 550\ 336.$$

Una de las dificultades para hallar más números perfectos era la poca disponibilidad de tablas de primos. En 1603, Pietro Cataldi[2], quien es recordado principalmente por su invención de la notación de las fracciones continuas, publicó una lista de primos menores que 5150. Por el procedimeinto directo de dividir por todos los primos que no exceden a la raíz cuadrada de un número, Cataldi determinó que $2^{17} - 1$ es primo, y en consecuencia

$$2^{16}(2^{17} - 1) = 8\ 589\ 869\ 056$$

es el sexto número perfecto.

Una pregunta que salta inmediatamente a la vista es si existen infinitos primos de la forma $2^p - 1$, donde p es primo. Si la respuesta fuese afirmativa, entonces existirían infinitos números perfectos (pares). Desafortunadamente ese es otro de los famosos problemas no resueltos.

Llega entonces el momento de demostrar el resultado anunciado sobre el dígitos final de los números perfectos pares.

Teorema 8.1.2

Todo número perfecto par n termina en los dígitos 6 u 8, es decir,

$$n \equiv 6(mod\ 10) \qquad o \qquad n \equiv 8(mod\ 10).$$

Demostración: Como n es perfecto par, se representa en la forma $n = 2^{k-1}(2^k - 1)$, donde $2^k - 1$ es primo. De acuerdo al lema anterior, el exponente k también es primo. Si $k = 2$, entonces $n = 6$ y se cumple la tesis del teorema. En el caso $k > 2$ se divide la demostración en dos partes según sea k de la forma $4m + 1$ ó $4m + 3$.

Si $k = 4m + 1$, entonces

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) \\ &= 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m \end{aligned}$$

Por inducción se comprueba que $16^t \equiv 6(mod\ 10)$ para todo entero positivo t. Aplicando la congruencia, se tiene

$$n \equiv 2 \cdot 6 - 6 \equiv 6(mod\ 10).$$

[2]Pietro Antonio Cataldi (1548-1626)

Ahora, en el caso $k = 4m + 3$, es

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m \end{aligned}$$

Usando nuevamente que $16^t \equiv 6(mod\ 10)$, se observa que

$$n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 86(mod\ 10).$$

Consecuentemente, todo número perfecto par n termina en los dígitos 6 u 8.**Q.e.d.**

Un análisis algo más profundo establece un mejor resultado, todo número perfecto par $n = 2^{k-1}(2^k - 1)$ termina siempre en los dígitos 6 ó 28. Como todo entero es congruente módulo 100 a sus dos últimos dígitos, basta probar que si $k = 4m + 3$, entonces $n \equiv 28(mod\ 100)$. Para ello note que

$$2^{k-1} \equiv 2^{4m+2} \equiv 16^m 4 \equiv 6 \cdot 4 \equiv 4(mod\ 10).$$

Más aún, para $k > 2$ se tiene que $4|2^{k-1}$, por lo que el número formado por los dos últimos dígitos de 2^{k-1} es divisible por 4. La situación es la siguiente: el último dígito de 2^{k-1} es es 4 y 4 divide a los dos últimos dígitos. Módulo 100, las posibilidades son

$$2^{k-1} = 4, 24, 44, 64, 84.$$

Pero ello implica que

$$2^k - 1 = 2 \cdot 2^{k-1} - 1 \equiv 7, 47, 87, 27 \text{ o } 67(mod\ 100),$$

de donde

$$n = 2^{k-1}(2^k - 1) \equiv 4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27 \text{ o } 84 \cdot 67(mod\ 100).$$

Dejamos al lector la comprobación de que todos los productos del miembro derecho son congruentes a 28 módulo 100.

Aunque no se ha encontrado ningún número perfecto impar, es posible dar algunas condiciones para su existencia. La más antigua se debe a Euler, quien demostró que si n es un número perfecto impar, entonces

$$n = p^\alpha q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_r^{2\beta_r},$$

donde $p, q_1, q_2, \ldots, q_r$ son primos impares diferentes y $p \equiv \alpha \equiv 1(mod\ 4)$.

TEOREMA 8.1.3 ***Euler***

Si n es un número perfecto impar, entonces

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r},$$

donde $p_1, p_2, \ldots, p_r$ son primos impares diferentes y $p_1 \equiv k_1 \equiv 1 (mod\ 4)$.

Demostración: Sea $n = p_1^{k_1} p_1^{k_2} p_2^{k_3} \cdots p_r^{k_r}$ la factorización prima de n. Como n es perfecto, podemos escribir

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r}).$$

Como n es impar, debe ser $n \equiv 1 (mod\ 4)$ o $n \equiv 3 (mod\ 4)$; en cualquier caso es $2n \equiv 2 (mod\ 4)$. Luego, $\sigma(n) = 2n$ es divisible por 2, pero no por 4. La implicación es que uno de los $\sigma(p_i^{k_i})$, digamos $\sigma(p_1^{k_1})$, tiene que ser par (pero no divisible por 4), mientras que los restantes $\sigma(p_i^{k_i})$ son enteros impares.

Para p_i se deben considerar dos casos: $p_i \equiv 1 (mod\ 4)$ y $p_i \equiv 3 (mod\ 4)$.

Si $p_i \equiv 3 \equiv -1 (mod\ 4)$, se tiene

$$\begin{aligned} \sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \ldots + p_i^{k_i} \\ &\equiv 1 + (-1) + (-1)^2 + \ldots + (-1)^{k_i} (mod\ 4) \\ &\equiv \begin{cases} 0 (mod\ 4) & \text{si } k_i \text{ es impar} \\ 1 (mod\ 4) & \text{si } k_i \text{ es par} \end{cases}. \end{aligned}$$

Como $\sigma(p_1^{k_1}) \equiv 2 (mod\ 4)$, ello indica que $p_1 \not\equiv 3 (mod\ 4)$, o de modo afirmativo $p_1 \equiv 1 (mod\ 4)$. Además, la congruencia $\sigma(p_i^{k_i}) \equiv 0 (mod\ 4)$ significa que 4 divide a $\sigma(p_i^{k_i})$, lo cual es imposible. En conclusión, si $p_i \equiv 3 (mod\ 4)$, para $i = 2, \ldots, r$, entonces su exponente k_i es un entero par.

Si fuera $p_i \equiv 1 (mod\ 4)$, lo cual es cierto para $i = 1$, entonces

$$\begin{aligned} \sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \ldots + p_i^{k_i} \\ &\equiv 1 + 1 + 1^2 + \ldots + 1^{k_i} (mod\ 4) \\ &\equiv k_i + 1 (mod\ 4). \end{aligned}$$

La condición $\sigma(p_1^{k_1}) \equiv 2 (mod\ 4)$ implica que $k_1 \equiv 1 (mod\ 4)$. Para los restantes valores de i sabemos que $\sigma(p_i^{k_i}) \equiv 1$ ó $3 (mod\ 4)$, y por tanto, $k_i \equiv 0$ ó $2 (mod\ 4)$. En todo caso k_i es un entero par. El punto crucial es que, independientemente de que sea $p_i \equiv 1 (mod\ 4)$ o $p_i \equiv 3 (mod\ 4)$, k_i es siempre par para $i \neq 1$. **Q.e.d.**

A partir de este teorema, todo número perfecto impar n puede ser expresado como

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r} = p_1^{k_1} \left(p_2^{j_2} \cdots p_r^{j_r}\right)^2 = p_1^{k_1} m^2.$$

Ello conduce directamente al siguiente corolario.

COROLARIO 8.1.1

Si n es un número perfecto impar, entonces n es de la forma

$$n = p^k m^2,$$

donde p es primo, $p \nmid m$ y $p \equiv k \equiv 1 (mod\ 4)$. En particular $n \equiv 1 (mod\ 4)$.

Demostración: Sólo la última afimración no es totalmente obvia. Como se tiene que $p \equiv 1 (mod\ 4)$, entonces $p^k \equiv 1 (mod\ 4)$. Note que m tiene que ser impar, es decir $m \equiv 1 (mod\ 4)$ ó $m \equiv 3 (mod\ 4)$, de donde $m^2 \equiv 1 (mod\ 4)$. Entonces

$$n = p^k m^2 \equiv 1 \cdot 1 \equiv 1 (mod\ 4),$$

lo cual demuestra el corolario. **Q.e.d.**

Otra línea de investigación se refiere a estimar el tamaño un número perfecto impar n. La cota inferior clásica fue obtenida por Turcaninov en 1908: n tiene al menos 5 factores primos diferentes y es mayor que $2 \cdot 10^6$. Con el advenimiento de las computadoras electrónicas, la cota inferior se ha elevado a $n > 10^{100}$. Todo ello soporta la creencia de que no existen números perfectos impares, pero sólo una demostración de su inexistencia sería concluyente. Estaríamos entonces en la curiosa posición de haber desarrollado toda una teoría para una clase inexistente de números.

El matemático Joseph Sylvester[3] escribió en 1888:

> "*Siempre se debe aplaudir la creencia de los geómetras griegos, de que habían tenido éxito al descubrir una clase de números, los cuales con toda probabilidad eran los únicos números perfectos*".

8.1.1. Ejercicios

1. Demuestre que $n = 2^{10}(2^{11} - 1)$ no es un número perfecto, comprobando que $\sigma(n) \neq 2n$. (Sugerencia: $2^{11} - 1 = 23 \cdot 89$.)

2. Demuestre las siguientes proposiciones:

   a) Ninguna potencia de primo puede ser un número perfecto.

[3] James Joseph Sylvester (1814-1897)

b) Un cuadrado perfecto no puede ser un número perfecto.

c) El producto de dos primos impares nunca es un número perfecto. (Sugerencia: desarrolle la desigualdad $(p-1)(q-1) > 2$ para obtener la relación $pq > p+q+1$.)

3. Si n es un número perfecto, demuestre que $\sum_{d|n} \frac{1}{d} = 2$.

4. Demuestre que todo número perfecto es un número triangular.

5. Si n es un número perfecto par ($n = 2^{k-1}(2^k - 1)$, demuestre que

$$n = 1 + 2 + 3 + \ldots + (2^k - l) \qquad \text{y} \qquad \phi(n) = 2^{k-1}(2^{k-1} - 1).$$

6. Para un número perfecto par $n > 6$, demuestre lo siguiente:

a) La suma de los dígitos de n es congruente a 1 módulo 9. (Sugerencia: la congruencia $2^6 \equiv 1(\mod 9)$ y el hecho de que todo primo $p \geq 5$ es de la forma $6k+1$ ó $6k+5$ implica que $n = 2^{p-1}(2^p - 1) \equiv 1(\mod 9)$.)

b) El entero n puede ser expresado como suma de cubos impares consecutivos. (Sugerencia: use el problema 1e) del capítulo I, sección 1, para establecer la identidad

$$1^3 + 3^3 + 5^3 + \ldots + (2^k - 1)^3 = 2^{2k-2}(2^{2k-1} - 1)$$

para todo $k \geq 1$.)

7. Muestre que ningún divisor de un número perfecto puede ser perfecto. (Sugerencia: aplique el resultado del problema 3.)

8. Halle los dos últimos dígitos del número perfecto $n = 2^{19936}(2^{19937} - 1)$.

9. Si $\sigma(n) = kn$ con $k \geq 3$, entonces el entero positivo n se llama *número k-perfecto* (o *múltiplemente perfecto*). Demuestre las siguientes proposiciones:

a) $523\ 776 = 2^9 3 \cdot 11 \cdot 31$ es 3-perfecto; $30\ 240 = 2^5 3^3 \cdot 5 \cdot 7$ es 4-perfecto; $14\ 182\ 439\ 040 = 2^7 3^4 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19$ es 5-perfecto.

b) Si n es un número 3-perfecto y $3 \nmid n$, entonces $3n$ es 4-perfecto.

c) Si n es un número 5-perfecto y $5 \nmid n$, entonces $5n$ es 6-perfecto.

d) Si $3n$ es un número $4k$-perfecto y $3 \nmid n$, entonces n es $3k$-perfecto.

10. Demuestre que los números 120 y 672 son los únicos números 3-perfectos de la forma $n = 2^k 3 \cdot p$, donde p es primo impar.

11. Un entero positivo n es *multiplicativamente perfecto* si n es igual al producto de todos sus divisores propios. En otras palabras,

$$n^2 = \prod_{d|n} d.$$

Encuentre todos los números multiplicativamente perfectos. (Sugerencia: note que $n^2 = n^{\tau(n)/2}$.)

12. Si $n > 6$ es un número perfecto par, demuestre que $n \equiv 4(\mod 6)$. (Sugerencia: $2^{p-1} \equiv 1(\mod 3)$ para todo primo impar p.)

13. La *media armónica* $H(n)$ de los divisores de un entero positivo n se define por la fórmula

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

Demuestre que si n es un número perfecto, entonces $H(n)$ tiene que ser entero. (Sugerencia: observe que $H(n) = \frac{n\tau(n)}{\sigma(n)}$.)

14. Los primos gemelos 5 y 7 son tales que la mitad de su suma es un número perfecto ¿Existen otros primos gemelos con es propiedad? (Sugerencia: dados los primos gemelos p y $p+2$ con $p > 5$, se tiene que $\frac{1}{2}(p+p+2) = 6k$ para cierto $k > 1$.)

15. Demuestre que si $2^k - 1$ es primo, entonces la suma

$$2^{k-1} + 2^k + 2^{k+1} + \ldots + 2^{k-2}$$

es un número perfecto. Por ejemplo, $2^3 - 1$ es primo y $2^2 + 2^3 + 2^4 = 28$ es perfecto.

16. Si n es un número perfecto, es decir, $n = 2^{k-1}(2^k - 1)$, demuestre que el producto de los divisores positivos de n es igual a n^k, es decir,

$$\prod_{d|n} d = n^k.$$

8.2. Números primos de Mersenne

Se ha hecho tradicional llamar a los números de la forma $M_n = 2^n - 1$ $(n \geq 1)$ **números de Mersenne** por el monje francés, Padre Marin Mersenne (1588- 1648), quien realizó una afirmación incorrecta pero provocativa sobre su primalidad. Los números de Mersenne que son primos se conocen como **primos de Mersenne**. Por lo visto en la sección anterior, la determinación de los primos de Mersenne, y en consecuencia de los números perfectos, se reduce al caso en que el mismo n es primo.

En el prefacio de su "Cogitata Physica-Mathematica" (1644), Mersenne afirmó que M_n es primo para $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ y compuesto para los restantes primos $p < 257$. Era obvio para otros matemáticos que Mersenne no pudo haber comprobado todos los números que anunció, pero nadie más pudo hacerlo. Euler verificó (1772) que M_{31} es primo, examinando todos los números primos hasta 46339 como posibles divisores, pero M_{67}, M_{127} y M_{257} se resistían a esa técnica. En este caso se trataba del octavo número perfecto

$$2^{30}(2^{31} - 1) = 2\ 305\ 843\ 008\ 139\ 952\ 128.$$

No fue hasta 1947, tras una tremenda labor apoyada por calculadoras mecánicas, que se completó el examen del carácter primo o compuesto de M_n para los 55 primos en el rango $p \leq 257$. Hoy se conoce que Mersenne cometió 5 errores: concluyó erróneamente que M_{67} y M_{257} eran primos, y excluyó a M_{61}, M_{89} y M_{107} de la lista de primos. Es asombroso que se hayan requerido más de 300 años para corregir al buen fraile.

En el estudio de los números de Mersenne, aparece un hecho extraño: si se sustituye cada uno de las cuatro primeros primos de Mersenne (3, 7, 31 y 127) en lugar de n en la fórmula $2^n - 1$ se obtiene un nuevo primo de Mersenne. Los matemáticos esperaban que ese procedimiento condujera a la obtención de un conjunto infinito de primos de Mersenne. En otras palabras, se conjeturó que si M_n es primo, entonces M_{M_n} era también primo. En 1953 una computadora de alta velocidad calculó

$$M_{M_{13}} = 2^{M_{13}} - 1 = 2^{8191} - 1$$

(un número de 2466 dígitos), que es compuesto.

Existen varios métodos para determinar cuándo ciertos tipos de números de Mersenne son primos o compuestos. A continuación se presenta uno de ellos.

Teorema 8.2.1

Si p y $q = 2p + 1$ son primos, entonces $q|M_p$ ó $q|M_p + 2$, pero q no divide a ambos a la vez.

Demostración: Del teorema de Fermat se conoce que

$$2^{q-1} - 1 \equiv 0(mod\ q),$$

y factorizando el miembro izquierdo es

$$\left(2^{\frac{q-1}{2}} - 1\right)\left(2^{\frac{q-1}{2}} + 1\right) = (2P - 1)(2^p + 1) \equiv 0(mod\ q).$$

Ello equivale a

$$M_p(M_p + 2) \equiv 0(mod\ q).$$

Por último, si fuera $q|M_p$ y $q|M_p+2$, se tendría $q|2$, lo que es imposible. **Q.e.d.**

Una sencilla aplicación basta para ilustrar este teorema. Si $p=23$, entonces el entero $q=2p+1=47$ es también primo, por lo que podemos considerar el caso M_{23}. La cuestión se reduce a determinar si $47|M_{23}$, o dicho de otro modo, si $2^{23}\equiv 1(mod\ 47)$. Ahora, se tiene que

$$2^{23}=2^3(2^5)^4\equiv 2^3(-15)^4(mod\ 47).$$

Pero

$$(-15)^4=225^2\equiv(-10)^2\equiv 6(mod\ 47).$$

De esas congruencias se deduce que

$$2^{23}\equiv 2^3 6\equiv 48\equiv 1(mod\ 47),$$

por lo que M_{23} es compuesto.

Nótese que este teorema no ayuda a encontrar la primalidad de M_{29}. En ese caso $59\nmid M_{29}$, pero $59|M_{29}+2$.

De las posibilidades $q|M_p$ ó $q|M_p+2$, es razonable preguntar ¿qué condiciones de q garantizan que $q|M_p$?

TEOREMA 8.2.2

Si $q=2n+1$ es primo, entonces

(1) $q|M_n$ si $q\equiv 1(mod\ 8)$ o $q\equiv 7(mod\ 8)$;

(2) $q|M_n+2$ si $q\equiv 3(mod\ 8)$ o $q\equiv 3(mod\ 8)$.

Demostración: Decir que $q|M_n$ es equivalente a que

$$2^{\frac{q-1}{2}}=2^2\equiv 1(mod\ q).$$

En términos del símbolo de Legendre, ello implica que

$$\left(\frac{2}{q}\right)=1.$$

Pero ya se conoce que ello es cierto si $q\equiv 1(mod\ 8)$ ó $q\equiv 7(mod\ 8)$. La demostración de (2) es análoga. **Q.e.d.**

Veamos una consecuencia inmediata de este teorema.

COROLARIO 8.2.1

Si p y $q=2p+1$ son primos con $p\equiv 3(mod\ 4)$, entonces $q|M_p$.

Demostración: Un primo impar p es de la forma $4k+1$ o $4k+3$. Si $p = 4k+3$, entonces $q = 8k+7$, por lo que $q|M_p$. En el caso $p = 4k+1$, se tiene $q = 8k+3$, de modo que $q \nmid M_p$. **Q.e.d.**

A continuación se muestra una lista de primos $p \equiv 3(mod\ 4)$, para los cuales el entero $q = 2p+1$ es también primo:

$$p = 11, 23, 83, 131, 179, 181, 239, 251.$$

En todos los casos M_p es compuesto.

Explorando más a fondo la situación, se presentan a continuación dos resultados de Fermat que restringen los divisores de M_p.

TEOREMA 8.2.3

Si p es primo impar, entonces todo divisor de M_p es de la forma $2kp+1$.

Demostración: Sea q un divisor primo cualquiera de M_p, tal que $2^p \equiv 1(mod\ q)$. Si $ord_q 2 = k$ (es decir, k es el menor entero positivo tal que $2^k \equiv 1(mod\ q)$), entonces conocemos que $k|p$. El caso $k = 1$ no es posible, pues entonces sería $q|1$. Luego, $k = p$, por ser p primo.
De acuerdo al teorema de Fermat, se tiene que $2^{q-1} \equiv 1(mod\ q)$, de donde se deduce que $k|q-1$. Como $k = p$, entonces $p|q-1$. Para culminar, sea $q-1 = pt$, es decir, $q = pt+1$. La demostración se completa al notar que si t fuera impar, entonces q tendría que ser par y se produce una contradicción. Así se tiene $q = 2kp+1$ para cierto k, lo que da a q la forma requerida. **Q.e.d.**

El teorema siguiente presenta una criba para eliminar posibles divisores de M_p.

TEOREMA 8.2.4

Si p es primo impar, entonces todo divisor primo q de M_p es de la forma $q \equiv \pm 1(mod\ 8)$.

Demostración: Sea $q = 2n+1$ un divisor primo de M_p. Si $a = 2^{\frac{p+1}{2}}$, entonces

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

Elevando a la potencia n la congruencia $a^2 \equiv 2(mod\ q)$, se obtiene

$$a^{q-1} = a^{2n} \equiv 2^n(mod\ q).$$

Como q es impar, se cumple $(a, q) = 1$, de donde $a^{q-1} \equiv 1(mod\ q)$. Las dos últimas congruencias nos dicen que $2^n \equiv 1(mod\ q)$, o dicho de otro modo, $q|M_n$. Aplicando ahora el teorema se obtiene la conclusión $q \equiv \pm 1(mod\ 8)$. **Q.e.d.**

Para ilustrar la utilización de esos teoremas, estudiemos M_{17}. Los enteros de la forma $34k + 1$, que son menores que $362 < \sqrt{M_{17}}$, son

$$35, 69, 103, 137, 171, 205, 239, 273, 307, 341.$$

Como el menor divisor (no trivial) de M_{17} tiene que ser primo, sólo se necesita considerar los primos entre los diez números anteriores, a saber,

$$103, 137, 239, 307.$$

El trabajo se simplifica al comprobar que $307 \not\equiv \pm 1 (mod\ 8)$, por lo que 307 puede ser borrado de la lista. Ahora, o M_{17} es primo, o uno de los tres números que quedan en la lista lo dividen. Con un poco de cálculo se puede comprobar que M_{17} no es divisible por ninguno de los números 103, 137 o 239. Resulta entonces que M_{17} es primo.

Luego de aparecer el octavo número perfecto $2^{30}(2^{31} - 1)$, Barlow, a partir de su tamaño, concluyó en su libro "Theory of Numbers" (publicado en 1811) que

> "*es el mayor que jamás será descubierto, pues siendo más curioso que útil, no es de esperar que alguna persona intente encontrar otro mayor*".

Lo que se puede afirmar es que Barlow subestimó la obstinada curiosidad humana.

8.2.1. Ejercicios

1. Demuestre que el número de Mersenne M_{13} es primo, por lo que $n = 2^{12}(2^{13} - 1)$ es perfecto. (Sugerencia: como $\sqrt{M_{13}} < 91$, los únicos candidatos a divisores primos de M_{13} son 53 y 79.)

2. Demuestre que el número de Mersenne M_{19} es primo, por lo que $n = 2^{18}(2^{19} - 1)$ es perfecto. (Sugerencia: los únicos divisores primos a probar son 191, 457 y 647.)

3. Demuestre que el número de Mersenne M_{29} es compuesto.

4. Un entero positivo n se dice **deficiente** si $\sigma(n) < 2n$ y **abundante** si $\sigma(n) > 2n$. Demuestre las siguientes proposiciones:

   a) Existen infinitos números deficientes. (Sugerencia: considere los enteros $n = pk$, donde p es primo impar y $k \geq 1$.)

   b) Existen infinitos números abundantes. (Sugerencia: considere los enteros $n = 2^k 3$, donde $k \geq 1$.)

   c) Existen infinitos números abundantes impares. (Sugerencia: considere los enteros $n = 945k$, donde k un entero positivo no divisible por 2, 3, 5 ó 7; como $945 = 3^3 5 \cdot 7$, es $(945, k) = 1$, de donde $\sigma(n) = \sigma(945)\sigma(k)$.)

5. Si n es un número perfecto par y $d|n$, con $1 < d < n$, demuestre que d es deficiente.

6. Demuestre que todo múltiplo de un número perfecto es abundante.

7. Una **pareja de números amigos** es un par de enteros positivos m, n que cumplen
$$\sigma(m) = m + n = \sigma(n).$$
Hasta la fecha se conocen al menos 900 parejas de números amigos, ninguna de las cuales son primos relativos. Confirme que las siguientes parejas de enteros constituyen números amigos:

   a) $220 = 2^2 5 \cdot 11$ y $284 = 2^2 \cdot 71$ (Pythagoras, 500 A.C.);

   b) $17296 = 2^4 \cdot 23 \cdot 47$ y $18416 = 2^4 \cdot 1151$ (Fermat, 1636);

   c) $9363584 = 2^7 \cdot 191 \cdot 383$ y $9437056 = 2^7 \cdot 73727$ (Descartes,1638).

8. Para una pareja de números amigos m, n, demuestre que
$$\left(\sum_{d|m} \frac{1}{d}\right)^{-1} + \left(\sum_{d|n} \frac{1}{d}\right)^{-1} = 1.$$

9. Demuestre las siguientes proposiciones:

   a) Ni p, ni p^2 pueden formar parte de una pareja de números amigos, si p es primo.

   b) El mayor entero en una pareja de números amigos es un número deficiente.

   c) Si m, n son una pareja de números amigos con m par y n impar, entonces n es un cuadrado perfecto. (Sugerencia: si p es primo impar, entonces $1 + p + p^2 + \ldots + p^k$ es impar sólo cuando k es par.)

10. En 1886, un joven italiano de 16 años anunció que $1184 = 2^5 37$ y $1210 = 2 \cdot 5 \cdot 11^2$ forman una pareja de números amigos, pero no indicó el método utilizado. Compruebe su afirmación.

11. La pareja de números amigos 220 y 284 representan el caso $n = 2$ de la siguiente regla debida a Tabit ibn Kurra, un matemático árabe del siglo IX: si $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ y $r = 9 \cdot 2^{2n-1} - 1$ son todos primos con $n \geq 2$, entonces $2^n pq$ y $2^n r$ forman una pareja de números amigos. Demuestre esa regla y verifique que $n = 4$ y $n = 7$ también producen parejas de números amigos.

12. Se entiende por **terna de números amigos** a tres enteros tales que la suma de dos cualesquiera de ellos es igual a la suma de los divisores propios del tercero. Compruebe que $2^5 \cdot 3 \cdot 13 \cdot 293 \cdot 337$, $2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 16561$ y $2^5 \cdot 3 \cdot 13 \cdot 99371$ forman una terna de números amigos.

13. Una sucesión finita de enteros positivos se dice **cadena sociable** si cada uno es la suma de los divisores propios del entero precedente (se considera que el último entero precede al primeo en la cadena). Compruebe que los siguientes enteros forman una cadena sociable:

$$14288, 15472, 14536, 14264, 12496.$$

Sólo se conocían dos cadenas sociables hasta 1970, cuando se encontraron nueve cadenas de cuatro enteros cada una.

14. Demuestre que

a) todo número perfecto impar n puede ser representado en la forma $n = pa^2$ con p primo;

b) si $n = pa^2$ es un número perfecto impar, entonces $n \equiv p(\mod 8)$.

15. Si n es un número perfecto impar, demuestre que n tiene al menos tres factores primos diferentes. (Sugerencia: asuma $n = p^k q^{2j}$, donde $p \equiv k \equiv 1(\mod 4)$ y use la desigualdad $2 = \frac{\sigma(n)}{n} \leq \left[\frac{p}{p-l}\right]\left[\frac{q}{q-1}\right]$ para llegar a una contradicción.)

16. Si el entero $n > 1$ es un producto de primos de Mersenne diferentes, demuestre que $\sigma(n) = 2^k$ para cierto k.

8.3. El famoso Teorema de Fermat

8.3.1. Ternas pitagóricas

Fermat, a quien muchos consideran el padre de la Teoría de Números modena, nunca hizo nada para asignarse ese papel. Publicó muy poco personalmente y prefería comunicar sus descubrimientos en cartas a sus amigos (usualmente con no más que una corta afirmación de que poseía la demostración) o mantener las notas guardadas. Cierto número de esas notas fueron escritas al margen de la traducción de Bachet de la "Arithmetica" de Diophanto. El más famoso de esos comentarios al margen es uno - presumiblemente escrito en 1637- que plantea:

> "*Es imposible escribir un cubo como suma de dos cubos, un bicuadrado como suma de dos bicuadrados y, en general, cualquier potencia mayor que dos como suma de dos potencias similares. He descubierto una demostración verdaderamente maravillosa para esto, pero este margen es muy estrecho para contenerla.*"

En esta nota, Fermat simplemente afirmaba que si $n > 2$, entonces la ecuación diofántica

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

no tiene solución en los enteros, a no ser la trivial, donde al menos una de las variables es cero.

Esta nota se ha hecho conocida como **Último Teorema de Fermat o Conjetura de Fermat**. Todos los resultados que enunció al margen de la "Arithmetica" fueron demostrados posteriormente excepto el Último Teorema, que solo pudo ser demostrado a finales del siglo XX por el matemático británico Andrew Wiles con técnicas nada elementales.

Sin embargo, Fermat dejó una prueba de su Último Teorema para el caso $n = 4$. Para poder desarrollar el argumento, primeramente trataremos de identificar todas las soluciones en los enteros positivos de la ecuación

$$x^2 + y^2 = z^2. \tag{8.1}$$

Como la longitud z de la hipotenusa de un triángulo rectángulo está relacionada con las longitudes x e y de los catetos por la famosa identidad pitagórica $x^2 + y^2 = z^2$, la búsqueda de todos los enteros positivos que satisfacen (8.1) es equivalente al problema de encontrar todos los triángulos rectángulos de lados enteros. El segundo problema fue desarrollado en tiempos de los babilonios y era un favorito de las antiguos geómetras griegos. Pitágoras mismo recibió el crédito por una fórmula para infinitos triángulos de ese tipo, a saber

$$\left\{ \begin{array}{rcl} x & = & 2n+1 \\ y & = & 2n^2+2n \\ z & = & 2n^2+2n+1 \end{array} \right. ,$$

donde n es un entero positivo. Esta fórmula no es válida para todos los triángulos rectángulos de lados enteros y no fue hasta que Euclides escribió "Los Elementos" que apareció la solución completa del problema.

La siguiente definición constituye una forma consisa de referirse a las soluciones de (8.1).

Definición 8.3.1

*Una **terna pitagórica o trío pitagórico** es un conjunto de tres enteros x, yz tales que*

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

*la terna se dice **primitiva** si $(x, y, z) = 1$.*

Quizás los ejemplos más conocidos de ternas pitagóricas sean $3, 4, 5$ y $5, 12, 13$, mientras que uno menos obvio es $12, 35, 37$.

Se deben resaltar varios puntos. Supongamos que x, y, z es una terna pitagórica y $d = (x, y, z)$. Haciendo $x = dx_1$, $y = dy_1$, $z = dz_1$, es fácil ver que

$$x_1^2 + y_1^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = z_1^2.$$

Es decir, x_1, y_1, z_1 forman una terna pitagórica primitiva. Luego, basta ocuparse de buscar todas las ternas pitagóricas primitivas, pues todas las ternas pitagóricas se obtienen al multiplicar estas por enteros no nulos. La búsqueda se confinará a los enteros positivos, ya que los negativos se obtienen a partir de estos por un simple cambio de signo.

Nuestro desarrollo requiere de dos lemas preparatorios.

LEMA 8.3.1 *Si x, y, z es una terna pitagórica primitiva, entonces x e y tienen diferente paridad.*

Demostración: Si x e y son pares, entonces $2|x^2 + y^2$, es decir $2|z^2$. De aquí que $(x, y, z) \geq 2$, lo cual es imposible. Por otra parte, si x e y son impares, entonces $x^2 \equiv 1(mod\ 4)$ y $y^2 \equiv 1(mod\ 4)$, de donde $z^2 = x^2 + y^2 \equiv 2(mod\ 4)$. Pero eso contradice que el cuadrado de todo entero es congruente a 0 ó a 1 módulo 4.**Q.e.d.**

Dado un trío pitagórico primitivo x, y, z, exactamente uno de esos enteros es par y los otros dos restantes son impares (pues $x^2 + y^2$ es impar). El lema anterior indica que el número par es x o y, por ello, a partir de ahora se consideran las ternas pitagóricas de modo que x es par, mientras que y y z son impares.

Es importante notar (y se tendrá en cuenta ese hecho) que toda pareja de los enteros x, y y z tienen que ser primos relativos. En efecto, si fuera $(x, y) = d > 1$, existiría un número primo p tal que $p|d$. Como d es divisor común de x e y, también lo es p, y por tanto $p|x^2$ y $p|y^2$. Pero entonces $p|z^2 = x^2 + y^2$, por lo que $p|z$. Ello contradice el heho de que $(x, y, z) = 1$, por lo que $d = 1$. De manera análoga se verifica que $(y, z) = (x, z) = 1$.

Por el lema anterior, no existe ninguna terna pitagórica cuyos elementos sean todos primos. Existen ternas pitagóricas en las que z y x o y son primos, por ejemplo $3, 4, 5$; $11, 60, 61$ y $19, 180, 181$. No se conoce si existen infinitas ternas de esa forma.

El siguiente paso necesario en el camino es establecer que si a y b son primos relativos positivos, de modo que su producto es un cuadrado, entonces a y b son cuadrados. Con apoyo del teorema fundamental de la Aritmética se puede demostrar mucho más, como indica el siguiente lema.

LEMA 8.3.2

Si $ab = c^n$ con $(a, b) = 1$, entonces a y b son potencias n-ésimas, es decir, existen enteros positivos a_1 y b_1 talles que $a = a_1^n$ y $b = b_1^n$.

Demostración: Sin perder generalidad, sean $a > 1$ y $b > 1$. Si

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad \text{y} \quad b = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

son las factorizaciones primas de a y b, entonces, como $(a, b) = 1$, los p_i son diferentes de los q_j. Como resultado, la factorización prima de ab es

$$ab = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}.$$

Si la factorización de c es $c = u_1^{l_1} u_2^{l_2} \cdots u_t^{l_t}$, entonces la condición $ab = c^n$ se expresa como

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s} = u_1^{nl_1} u_2^{nl_2} \cdots u_t^{nl_t}.$$

Así los primos $u_1, u_2, \ldots, u_t$ son (en cierto orden) $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ y los exponentes $nl_1, nl_2, \ldots, nl_t$ son los correspondientes $k_1, k_2, \ldots, k_r, j_1, j_2, l \ldots, j_s$. En conlusión, cada uno de los enteros k_i y j_i tiene que ser divisible por n. Haciendo ahora

$$\begin{aligned} a_1 &= p_1^{\frac{k_1}{n}} p_2^{\frac{k_2}{n}} \cdots p_r^{\frac{k_r}{n}} \\ b_1 &= q_1^{\frac{j_1}{n}} q_2^{\frac{j_2}{n}} \cdots q_s^{\frac{j_s}{n}}, \end{aligned}$$

entonces $a_1^n = a$ y $b_1^n = b$, que es lo que se quería demostrar. **Q.e.d.**

Con esta preparación, ya estamos listos para la caracterización de las ternas pitagóricas primitivas.

TEOREMA 8.3.1

Todas las soluciones de la ecuación pitagórica

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

que satisfacen las condiciones

$$(x, y, z) = 1, \quad 2|x, \quad , x > 0, \ y > 0, \ z > 0,$$

están dadas por las fórmulas

$$\begin{cases} x &= 2st \\ y &= s^2 - t^2 \\ z &= s^2 + t^2 \end{cases},$$

para enteros $s > t > 0$ tales que $(s, t) = 1$ y $s \not\equiv t (mod\ 2)$.

Demostración: Sea x, y, z una terna pitagórica (positiva) primitiva. Como se acordó que x es par y y y z son impares, $z-y$ y $z+y$ son pares. Sean $z-y=2u$ y $x+y=2v$. Ahora se puede reescribir la ecuación $x^2+y^2=z^2$ en la forma

$$x^2 = z^2 - y^2 = (z-y)(z+y),$$

de donde

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = uv.$$

Nótese que u y v son primos relativos. En efecto, si $(u,v)=d>1$, entonces $d|(u-v)$ y $d|(u+v)$, o lo que es lo mismo, $d|y$ y $d|z$, lo que contradice el hecho de que $(y,z)=1$. Tomando en consideración el lema 8.3.2, se concluye que u y v son cuadrados perfectos, es decir,

$$u = s^2, \qquad v = t^2,$$

donde s y t son enteros positivos. Sustituyendo ahora se tiene

$$\left\{\begin{array}{rcccl} z & = & u+v & = & s^2+t^2 \\ y & = & u-v & = & s^2-t^2 \\ x^2 & = & 4uv & = & 4s^2t^2 \quad \Rightarrow \quad x = 2st \end{array}\right. .$$

Como cualquier factor común de s y t dividiría también a y y z, tiene que ser $(s,t)=1$. Resta observar que si s y t tiene igual paridad, entonces x e y serían pares, lo cual es imposible. Luego, s y t tienen diferente paridad, es decir, $s \not\equiv t (mod\ 2)$.

Recíprocamente, sean s y t dos enteros sujetos a las condiciones anteriormente descritas y sean

$$\left\{\begin{array}{rcl} x & = & 2st \\ y & = & s^2-t^2 \\ z & = & s^2+t^2 \end{array}\right. .$$

Resulta fácil comprobar que estos números forman una terna pitagórica, pues

$$x^2+y^2 = (2st)^2 + (s^2-t^2)^2 = (s^2+t^2)^2 = z^2.$$

Para comprobar que la terna es primitiva, asumamos que $(x,y,z)=d>1$ y sea p un divisor primo de d. Como z es impar, tiene que ser $p \neq 2$. De $p|y$ y $p|z$ se obtiene que $p|(z+y)$ y $p|(z-y)$, es decir, $p|2s^2$ y $p|2t^2$. Pero entonces p es divisor común de s y t, lo cual es incompatible con $(s,t)=1$. Luego, $d=1$ y la terna pitagórica x, y, z es primitiva. **Q.e.d.**

La tabla a continuación muestra algunas ternas pitagóricas primitivas, a partir de valores pequeños de s y t. Para cada $s=1,2,3,\ldots,7$, se han seleccionado los valores

de t que son primos relativos con s, menores y con diferente paridad que s.

s	t	$x = 2st$	$y = s^2 - t^2$	$z = s^2 - t^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85

Partiendo de ésta o de otra tabla más extensa, el lector podría sospechar que si x, y, z es una terna pitagórica primitiva, entonces exactamente uno de los enteros x o y es divisible por 3. Ese es, de hecho, el caso. En efecto, por el teorema 8.3.1 es

$$\begin{cases} x &= 2st \\ y &= s^2 - t^2 \\ z &= s^2 + t^2 \end{cases},$$

donde $(s,t) = 1$. Si $3|s$ o $3|t$, evidentemente $3|x$. En otro caso ($3 \nmid s$ y $3 \nmid t$) el teorema de Fermat afirma que

$$s^2 \equiv 1(mod\ 3), \qquad t^2 \equiv 1(mod\ 3)$$

y por tanto

$$y = s^2 - t^2 \equiv 0(mod\ 3).$$

Se llama **triángulo pitagórico** al triángulo rectángulo cuyos lados tienen longitudes enteras. El siguiente teorema muestra un hecho geométrico interesante respecto a estos triángulos.

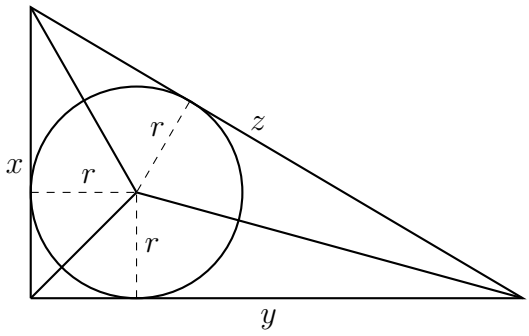
Teorema 8.3.2

El radio del círculo inscrito en un triángulo pitagórico es siempre entero.

Demostración: Sea r el radio del círculo inscrito en un triángulo de hipotenusa z y catetos x e y. El área del triángulo es igual a la suma de las áreas de los tres triángulos que tienen vértice común en el centro del círculo, entonces

$$\frac{1}{2}xy = \frac{1}{2}rx + \frac{1}{2}ry + \frac{1}{2}rz = \frac{1}{2}r(x + y + z).$$

La situación se ilustra a continuación.



Ahora, $x^2 + y^2 = z^2$. Pero se sabe que las soluciones enteras positivas de esa ecuación están dadas por

$$\left\{ \begin{array}{rcl} x & = & 2kst \\ y & = & k(s^2 - t^2) \\ z & = & k(s^2 + t^2) \end{array} \right. ,$$

para una selección apropiada de los enteros k, s, t. Sustituyendo x, y, z en la ecuación $xy = r(x + y + z)$ y despejando r, se obtiene

$$\begin{array}{rcl} r & = & \dfrac{2k^2st(s^2 - t^2)}{k(2st + s^2 - t^2 + s^2 + t^2)} \\ & = & \dfrac{kt(s^2 - t^2)}{s + t} = kt(s - t), \end{array}$$

que es entero. **Q.e.d.**

Aprovechamos la oportunidad para mencionar otro resultado relativo a los triángulos pitagóricos. Note que es posible que diferentes triángulos pitagóricos tengan la misma área, por ejemplo, los triángulos rectángulos asociados a las ternas pitagóricas $20, 21, 29$ y $12, 35, 57$ tienen área igual a 210. Fermat demostró que para todo entero $n > 1$ existen n triángulos pitagóricos con hipotenusa diferentes e igual área. se omiten los detalles de la demostración.

8.3.2. Ejercicios

1. *a*) Halle tres ternas pitagóricas diferentes, no necesariamente primitivas, de la forma $16, y, z$.

   b) Obtenga todas las ternas pitagóricas primitivas x, y, z con $x = 40$ y con $x = 60$.

2. Si x, y, z es una terna pitagórica primitiva, demuestre que $x + y$ y $x - y$ son congruentes módulo 8 a 1 ó a 7.

3. *a*) Demuestre que si $n \equiv 2(\mod 4)$, entonces existe una terna pitagórica primitiva x, y, z con $x = n$ ó $y = n$.

b) Si $n > 3$ es arbitrario, halle una terna pitagórica (no necesariamente primitiva) que contenga a n como una de sus miembros. (Sugerencia: para n impar, considere la terna $n, \frac{1}{2}(n^2-1), \frac{1}{2}(n^2+1)$; para n par, considere la terna $n, \frac{n^2}{4}-1, \frac{n^2}{4}+1$.)

4. Demuestre que en una terna pitagórica primitiva x, y, z el producto xy es divisible por 12, por lo que $60|xyz$.

5. Para un entero positivo n dado, demuestre que existen al menos n ternas pitagóricas con el mismo primer miembro. (Sugerencia: sea $y_k = 2^k(2^{2n-2k}-1)$ y $z_k = 2^k(2^{2n-2k}+1)$ para $k = 0, 1, 2, \ldots, n-1$; entonces $2^{n+1}, y_k, z_k$ son ternas pitagóricas.)

6. Compruebe que $3, 4, 5$ es la única primitiva terna pitagórica con enteros consecutivos.

7. Demuestre que $3n, 4n, 5n$ con $n = 1, 2, \ldots$ son la únicas ternas pitagóricas cuyos términos están en progresión aritmética. (Sugerencia: denote a la terna en cuestión por $x-d, x, x+d$ y resuelva para x en términos de d.)

8. Encuentre todos los triángulos pitagóricos cuya área coincide con su perímetro. (Sugerencia: las ecuaciones $x^2+y^2=z^2$ y $x+y+z=\frac{1}{2}xy$ implican que $(x-4)(y-4)=8$.)

9. *a*) Demuestre que si x, y, z es una terna pitagórica primitiva, donde x y z son enteros consecutivos, entonces

$$\begin{cases} x &= 2t(t+1) \\ y &= 2t+1 \\ z &= 2t(t+1)+1 \end{cases},$$

para cierto $t > 0$. (Sugerencia: la ecuación $1 = z - x = s^2 + t^2 - 2st$ implica que $s - t = 1$.)

b) Demuestre que si $x, .y, z$ es una terna pitagórica primitiva con $z - y = 2$, entonces

$$\begin{cases} x &= 2t \\ y &= t^2-1 \\ z &= t^2+1 \end{cases},$$

para cierto $t > 1$.

10. Demuestre que existen infinitas ternas pitagóricas primitivas x, y, z cuyo miembro par x es un cuadrado perfecto. (Sugerencia: considere la terna $4n^2$, n^4-4, n^4+4, donde n es un entero impar cualquiera.)

11. Para un entero positivo cualquiera n, demuestre que existe un triángulo pitagórico tal que el radio del círculo inscrito es n. (Sugerencia: si r es el radio del círculo inscrito en el triángulo pitagórico de catetos a, b e hipotenusa c, entonces $r = \frac{1}{2}(a + b - c)$; considere la terna $2n + 1, 2n^2 + 2n, 2n^2 + 2n + 1$.)

12. *a*) Demuestre que existen infinitas ternas pitagóricas primitivas x, y, z en las que x e y son enteros consecutivos. Muestre tres de ellas. (Sugerencia: si $x, x + 1, z$ forman una terna pitagórica, entonces también lo es la terna $3x + 2z + 1, 3x + 2z + 2, 4x + 3z + 2$.)

    b) Demuestre que existen infinitas ternas pitagóricas x, y, z en las que x e y son números triangulares consecutivos. Muestre tres de ellas. (Sugerencia: si $x, x + 1, z$ forman una terna pitagórica, entonces también lo es la terna $t_{2x}, t_{2x+1}, (2x + 1)z$.)

13. Use el problema 12 para demostrar que existen infinitos números triangulares que son cuadrados perfectos. Muestre cinco de ellos. (Sugerencia: si $x, x + 1, z$ forman una terna pitagórica, entonces haciendo $u = z - x - 1$, $v = x + \frac{1}{2}(1 - z)$, se obtiene $\frac{u(u+1}{2} = v^2$.)

8.3.3. El prńcipe de los aficionados

Ningún período ha sido tran fructífero para la Matemática como el siglo XVII, sólo Europa del Norte produjo tantos hombres de habilidades sobresalientes como los que existieron durante todo el milenio precedente. En esa época se hace famoso un abogado francés aficionado a la Matemática, Pierre de Fermat (1601-1665). Fermat, el "Príncipe de los aficionados", fue el sin dudas un gran matemático que siguió el tema de modo paralelo a una carrera no científica. Abogado de profesión y magistrado adjunto del parlamento provincial de Toulouse, no tenía un entrenamiento matemático particular.

Hoy se reconoce a Fermat como uno de los inventores de la Geometría Analítica junto a René Descartes[4], propuso bases técnicas del cálculo diferencial e integral, y con Pascal estableció las bases conceptuales de la Teoría de Probabilidades. Pero su área preferida fue sin dudas la Teoría de Números, donde sus contribuciones opacan cualquier otra.

Fermat prefería el placer derivado de la investigación matemática y se negó siempre a publicar sus resultados. En compensación por su falta de interés en publicar, mantuvo una voluminosa correspondencia con matemáticos contemporáneos. Por otra parte, acostumbraba insertar notas en los márgenes de los libros que leía. La copia personal de Fermat de la traducción de Bachet de la "Arithmetica" de Diofanto contiene en sus márgenes varios de los más famosos teoremas de la Teoría de Números, entre

[4]René Descartes (1596-1650)

los que destaca el **Último Teorema**. Eso fue descubierto 5 años tras la muerte de Fermat por su hijo Samuel, quien hizo una nueva edición de la "Arithmetica" incorporándole los celebrados márgenes de su padre, entre ellos el famoso

> "*Es imposible escribir un cubo como suma de dos cubos, un bicuadrado como suma de dos bicuadrados y, en general, cualquier potencia mayor que dos como suma de dos potencias similares. He descubierto una demostración verdaderamente maravillosa para esto, pero este margen es muy estrecho para contenerla.*"

¡Qué bueno hubiese sido que la "Arithmetica" tuviese márgenes más anchos!

8.3.4. El "Último Teorema"

Con el conocimiento de las ternas pitagóricas, ya estamos preparados para estudiar el caso en que el mismo Fermat demostró su conjetura, el caso $n = 4$. La técnica utilizada es una forma de inducción llamada "**método del descenso infinito de Fermat**". Se asume que existe una solución del problema en los enteros positivos y a partir de ella se construye una nueva solución en enteros positivos menores, lo que conduce a otra nueva solución en enteros positivos aún menores y así sucesivamente. Como los enteros positivos no pueden decrecer indefinidamente, la suposición inicial tiene que ser falsa, por lo que no hay solución posible.

En lugar de dar la demostración de Fermat para el caso $n = 4$, se establece un hecho más fuerte, la imposibilidad de solucionar en los enteros positivos la ecuación

$$x^4 + y^4 = z^2.$$

TEOREMA 8.3.3

La ecuación diofántica

$$x^4 + y^4 = z^2$$

no tiene solución en enteros positivos x, y, z.

Demostración: Con la idea de obtener una contradicción, supongamos que existe una solución x_0, y_0, z_0 de $x^4 + y^4 = z^2$. No se pierde generalidad al suponer que $(x_0, y_0) = 1$. En efecto, en caso contrario se hace $(x_0, y_0) = d$ y sean $x_0 = x_1 d$, $y_0 = y_1 d$, $z_0 = z_1 d$, para obtener

$$x_1^4 + y_1^4 = z_1^2$$

con $(x_1, y_1) = 1$.

Al expresar la ecuación $x_0^4 + y_0^4 = z_0^2$ en la forma

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2,$$

se observa que x_0^2, y_0^2, z_0 constituyen una terna pitagórica primitiva y se puede aplicar el teorema 8.3.1. Como exactamente uno de los enteros x_0^2 o y_0^2 es par, supongamos que se trata de x_0^2 (por tanto x_0 es par). Entonces existen enteros primos relativos $s > t > 0$ tales que

$$\begin{cases} x_0^2 &= 2st \\ y_0^2 &= s^2 - t^2 \\ z_0 &= s^2 + t^2 \end{cases},$$

donde exactamente uno de los dos, s o t, es par. Si s es par, entonces

$$1 \equiv y_0^2 \equiv s^2 - t^2 \equiv 0 - 1 \equiv 3(mod\ 4),$$

lo cual es imposible. Luego s tiene que ser impar y, en consecuencia, t es par. Sea $t = 2r$, entonces es $x_0^2 = 4st$, lo que dice que

$$\left(\frac{x_0}{2}\right)^2 = sr.$$

Pero el lema 8.3.2 afirma que entonces s y r son cuadrados perfectos, es decir, $s = z_1^2$, $r = w_1^2$ para enteros positivos z_1, w_1.

Apliquemos ahora nuevamente el teorema 8.3.1 a la nueva ecuación

$$t^2 + y_0^2 = s^2.$$

Como $(s, t) = 1$, se tiene que $(t, y_0, s) = 1$, por lo que t, y_0, s es una terna pitagórica primitiva. Con t par, se obtiene

$$\begin{cases} t &= 2uv \\ y_0^2 &= u^2 - v^2 \\ s &= u^2 + v^2 \end{cases},$$

para enteros primos relativos $u > v > 0$. Pero la relación

$$un = \frac{t}{2} = r = w_1^2$$

significa que u y v son cuadrados; sean $u = x_1^2$ and $v = y_1^2$. Cuando esos valores se sustituyen en la ecuación para s se obtiene

$$z_1^2 = s = u^2 + v^2 = x_1^4 + y_1^4.$$

Un punto crucial es que, como z_1 y t son positivos, se tiene la desigualdad

$$0 < z_1 \leq z1^2 = s \leq s^2 \leq s^2 + t^2 = z_0.$$

Ha sucedido lo siguiente: a partir de una solución x_0, y_0, z_0 de $x^4 + y^4 = z^2$, se ha construido otra solución x_1, y_1, z_1 tal que $0 < z_1 < z_0$. Repitiendo el proceso indefinidamente se obtiene una sucesión decreciente infinita de enteros positivos

$$z_0 > z_1 > z_2 > \dots$$

Pero existe sólo una cantidad finita de enteros positivos menores que z_0, por lo que se obtiene una contradicción. Entonces $x^4 + y^4 = z^2$ no tiene solución en los enteros positivos. **Q.e.d.**

Como corolario inmediato se obtiene el siguiente.

COROLARIO 8.3.1

La ecuación diofántica

$$x^4 + y^4 = z^4$$

no tiene solución en enteros positivos x, y, z.

Demostración: Si x_0, y_0, z_0 fuera una solución positiva de $x^4 + y^4 = z^4$, entonces x_0, y_0, z_0^2 sería solución de $x^4 + y^4 = z^2$, lo cual es imposible. **Q.e.d.**

De $x^4 + y^4 = z^2$ se pasa a una ecuación diofántica similar, $x^4 - y^4 = z^2$. La prueba de su no solubilidad es similar a la del teorema 8.3.3, pero muestra una pequeña variación en el método del descenso infinito.

TEOREMA 8.3.4

La ecuación diofántica

$$x^4 - y^4 = z^2$$

no tiene solución en enteros positivos x, y, z.

Demostración: La demostración es por el absurdo. Supongamos que la ecuación admite solución en los enteros y sea x_0, y_0, z_0 una solución con el menor valor posible de x. En particular, esta suposición obliga a que x_0 sea impar (¿por qué?). Si $(x_0, y_0) = d > 1$, entonces haciendo $x_0 = x_1 d$ y $y_0 = y_1 d$ se obtiene $d^4(x_1^4 - y_1^4) = z_0^2$, de donde $d^2 | z_0$ o $z_0 = z_1 d^2$ para cierto $z_1 > 0$. Así se obtiene una solución x_1, y_1, z_1 de la ecuación tal que $0 < x_1 < x_0$, lo cual es imposible. Luego, podemos asumir que la solución x_0, y_0, z_0 es tal que $(x_0, y_0) = 1$. La demostración se separa ahora en dos casos en dependencia de que y_0 sea par o impar.

Sea y_0 un entero par. Si se escribe la ecuación $x_0^4 - y_0^4 = z_0^2$ en la forma

$$z_0^2 + (y_0^2)^2 = (x_0^2)^2,$$

se observa que z_0, y_0^2, x_0^2 constituyen una terna pitagórica. Entonces existen enteros primos relativos $s > t > 0$ tales que

$$\left\{ \begin{array}{rcl} z_0 & = & 2st \\ y_0^2 & = & s^2 - t^2 \\ x_0^2 & = & s^2 + t^2 \end{array} \right. .$$

Se cumple que

$$s^4 - t^4 = (s^2 + t^2)(s^2 - t^2) = (x_0 y_0)^2,$$

por lo que $s, t, x_0 y_0$ es una solución (positiva) de la ecuación $x^4 - y^4 = z^2$. Como

$$0 < s < \sqrt{s^2 + t^2} < x_0,$$

se obtiene una contradicción con la naturaleza minimal de x_0.

Sea ahora y_0 un entero impar. Usando las fórmulas de las terna pitagóricas primitivas es

$$\left\{ \begin{array}{rcl} y_0^2 & = & 2st \\ z_0 & = & s^2 - t^2 \\ x_0^2 & = & s^2 + t^2 \end{array} \right. ,$$

donde s es par y t es impar. Entonces en la relación $y_0^2 = 2st$, se tiene $(2s, t) = 1$, por lo que $2s$ y t son cuadrados perfectos, digamos, $2s = w^2$, $t = v^2$. Como w es par, hacemos $w = 2u$, de donde $s = 2u^2$. Entonces

$$x_0^2 = s^2 + t^2 = 4u^4 + v^4,$$

por lo que $2u^2, v^2, x_0$ forman una terna pitagórica primitiva, de modo que existen enteros $a > b > 0$ con $(a, b) = 1$ tales que

$$\left\{ \begin{array}{rcl} 2u^2 & = & 2ab \\ v^2 & = & a^2 - b^2 \\ x_0 & = & a^2 + b^2 \end{array} \right. .$$

La igualdad $u^2 = ab$ garantiza que a y b son cuadrados perfectos, es decir $a = c^2$ y $b = d^2$. A partir de este punto, el resto de la demostración es sencilla. En efecto, sustituyendo es

$$v^2 = a^2 - b^2 = c^4 - d^4.$$

El resultado es una nueva solución c, d, v de la ecuación $x^4 - y^4 = z^2$ tal que

$$0 < c = \sqrt{a} < a^2 + b^2 = x_0,$$

lo que contradice la minimalidad de x_0.

La única resolución de esas contradicciones es que la ecuación $x^4 - y^4 = z^2$ no puede tener solución en los enteros positivos. **Q.e.d.**

En el margen de su copia de la Arithmetica de Diofanto, Fermat enunció y demostró que el área de un triángulo rectángulo no puede ser el cuadrado de un número racional. Quitando las fracciones, ello se expresa en el siguiente teorema sobre triángulos pitagóricos.

Teorema 8.3.5

El área de un triángulo pitagórico no puede ser nunca un cuadrado perfecto.

Demostración: Consideremos el triángulo pitagórico, cuya hipotenusa tiene longitud z y cuyos catetos miden x e y, de modo que $x^2 + y^2 = z^2$. El área del triángulo es $\frac{1}{2}xy$ y si fuera un cuadrado, por ejemplo, u^2, se tendría $2xy = 4u^2$. Sumando y restando esta expresión de $x^2 + y^2 = z^2$ se obtiene

$$(x + y)^2 = z^2 + 4u^2 \qquad \text{y} \qquad (x - y)^2 = z^2 - 4u^2.$$

Multiplicando esas ecuaciones se tiene que la diferencia de dos potencias cuartas es un cuadrado

$$(x^2 - y^2)^2 = z^4 - 16u^4 = z^4 - (2u)^4.$$

Pero esto contradice el teorema 8.3.4, por lo que no puede existir un triángulo pitagórico, cuya área sea un cuadrado perfecto. **Q.e.d.**

Existen varios problemas simples sobre triángulos pitagóricos, que aún esperan por ser solucionados. El corolario 8.3.1 se puede expresar diciendo que no existe un triángulo pitagórico cuyos lados sean todos cuadrados. Sin embargo, no es difícil producir un triángulo pitagórico cuyos lados, incrementados en 1, sean todos cuadrados, por ejemplo; los triángulos asociados a las ternas

$$132 - 1, 102 - 1, 142 - 1 \quad \text{y} \quad 2872 - 1, 2652 - 1, 3292 - 1.$$

Una pregunta obvia -y hasta ahora sin respuesta- es si existe una cantidad infinita de esos triángulos. Se pueden encontrar triángulos pitagóricos cuyos lados sean todos números triangulares, es decir, números de la forma

$$t_n = \frac{n(n+1)}{2}.$$

Un ejemplo es el triángulo correspondiente a la terna $t_{132}, t_{143}, t_{164}$. No se sabe aún si existe una cantidad infinita de esos triángulos.

A pesar de que la conjetura de Fermat retó a los más famosos matemáticos por los últimos 300 años. Euler propuso la primera demostración de la conjetura de Fermat

para el primo $p = 3$ en 1770. El razonamiento estaba incompleto, pero Legendre lo completó más adelante. Usando el método del descenso infinito, Dirichlet y Legendre desarrollaron de manera independiente el caso $p = 5$ alrededor de 1825. El matemático alemán Kummer logró el mayor avance en 1843 al crear el concepto de número ideal y demostrando exitosamente la conjetura de Fermat para una clase grande de primos a los que llamó "**primos regulares**". La lucha por encontrar una demostración continuó y en 1908 la Academia de Ciencias de Gottingen destinó un premio de 100 000 marcos a la primera prueba completa de la conjetura de Fermat, cuyo resultado inmediato fue una avalancha de demostraciones incorrectas de matemáticos aficionados. Es así que la conjetura de Fermat se ha ganado la reputación de ser el problema matemático con una mayor cantidad de falsas demostraciones publicadas.

Muchos fueron los que dedicaron su tiempo e ingenio al intento. hasta que finalmente! en la última década del siglo XX Andrew Wiles logra demostrar el teorema, aplicando técnicas nada elementales que le llevó tres días exponer.

8.3.5. Ejercicios

1. Demuestre que la ecuación $x^2 + y^2 = z^3$ tiene infinitas soluciones para x, y, z enteros positivos. (Sugerencia: para todo $n > 3$, sea $x = n(n^2 - 3)$ y sea $y = 3n^2 - 1$.)

2. Demuestre el teorema: Las únicas soluciones en enteros no negativos de la ecuación $x^2 + 2y^2 = z^2$ con $(x, y, z) = 1$ están dadas por

$$\begin{cases} x &= \pm(2s^2 - t^2) \\ y &= 2st \\ z &= 2s^2 + t^2 \end{cases},$$

   donde s y t son enteros no negativos arbitrarios. (Sugerencia: si u, v, w son tales que $y = 2w$, $z + x = 2u$, $z - x = 2v$, entonces la ecuación se convierte en $2w^2 = uv$.)

3. En una terna pitagórica x, y, z, demuestre que no más de uno entre x, y, z puede ser un cuadrado perfecto.

4. Demuestre las siguientes proposiciones:

   a) El sistema de ecuaciones simultáneas

$$x^2 + y^2 = z^2 - 1 \qquad \text{y} \qquad x^2 - y^2 = w^2 - 1$$

   tiene infinitas soluciones en enteros positivos x, y, z, w. (Sugerencia: para todo entero $n \geq 1$, sea $x = 2n^2$ y $y = 2n$.)

b) El sistema de ecuaciones simultáneas

$$x^2 + y^2 = z^2 \qquad \text{y} \qquad x^2 - y^2 = w^2$$

no admite solución en enteros positivos x, y, z, w.

c) El sistema de ecuaciones simultáneas

$$x^2 + y^2 = z^2 + 1 \qquad \text{y} \qquad x^2 - y^2 = w^2 + 1$$

tiene infinitas soluciones en enteros positivos x, y, z, w. (Sugerencia: para todo entero $n \geq 1$, sea $x = 8n^4 + 1$ y $y = 8n^3$.)

5. Use el problema 4 para demostrar que no existe solución en enteros positivos de las ecuaciones simultáneas

$$x^2 + y^2 = z^2 \qquad \text{y} \qquad x^2 + 2y^2 = w^2.$$

(Sugerencia: toda solución del sistema satisface también que $z^2 + 2y^2 = w^2$ y $z^2 - y^2 = x^2$.)

6. Demuestre que no existe solución en enteros positivos de las ecuaciones simultáneas

$$x^2 + y^2 = z^2 \qquad \text{y} \qquad x^2 + z^2 = w^2.$$

Luego, no existen triángulos pitagóricos, cuya hipotenusa y uno de sus catetos formen los catetos de otro triángulo pitagórico. (Sugerencia: toda solución del sistema satisface también que $x^2 + (wy)^2 = z^4$.)

7. Demuestre que la ecuación $x^4 - y^4 = 2z^2$ no tiene solución en enteros positivos x, y, z. (Sugerencia: como x, y tienen que tener igual paridad, $x^2 + y^2 = 2a^2$, $x + y = 2b^2$, $x - y = 2c^2$ para ciertos a, b, c; luego, $a^2 = b^4 + c^4$.)

8. Verifique que la única solución en enteros positivos primos relativos de la ecuación $x^4 + y^4 = 2z^2$ es $x = y = z = 1$. (Sugerencia: la ecuación

$$z^4 - (xy)^4 = \left[\frac{x^4 - y^4}{2}\right]^2$$

también se satisface por toda solución de la ecuación dada.)

9. Demuestre que la ecuación diofántica $x^4 - 4y^4 = z^2$ no tiene solución en enteros positivos x, y, z. (Sugerencia: reescriba la ecuación como $(2y^2)^2 + z^2 = (x^2)^2$ y aplique el teorema 8.3.1.)

10. Use el problema 9 para demostrar que no existe un triángulo pitagórico cuya área sea el doble de un cuadrado perfecto. (Sugerencia: asuma por el contrario que $x^2 + y^2 = z^2$ y $\frac{1}{2}xy = 2w^2$; entonces $(x + y) = z^2 + 8w^2$ y $xy = 2w^2$, mientras que $(x - y) = z^2 - 8w^2$; ello implica que $z^4 - 4(2w)^4 = (x^2 - y^2)^2$.)

11. Demuestre el teorema: La única solución en enteros positivos de la ecuación

$$\frac{1}{x^2}+\frac{1}{y^2}=\frac{1}{z^2}$$

con $(x,y,z)=1$, está dada por

$$\left\{\begin{array}{rcl} x &=& 2st(s^2+t^2) \\ y &=& s^4-t^4 \\ z &=& 2st(s^2-t^2) \end{array}\right. ,$$

donde s,t son enteros positivos primos prelativos, uno de los cuales es par, con $s>t$.

12. Demuestre que la ecuación

$$\frac{1}{x^4}+\frac{1}{y^4}=\frac{1}{z^2}$$

no tiene solución en los enteros positivos.

8.4. Sumas de cuadrados

8.4.1. Suma de dos cuadrados

Históricamente, un problema que ha recibido gran atención es el de la representación de números como suma de cuadrados. En este capítulo desarrollaremos el material suficiente para responder totalmente la pregunta ¿cuál es el menor valor n, de modo que todo entero positivo puede ser escrito como suma de no más de n cuadrados? Tras examinar los primeros enteros positivos,

$$\begin{array}{rcl} 1 &=& 1^2 \\ 2 &=& 1^2+1^2 \\ 3 &=& 1^2+1^2+1^2 \\ 4 &=& 2^2 \\ 5 &=& 2^2+1^2 \\ 6 &=& 2^2+1^2+1^2 \\ 7 &=& 2^2+1^2+1^2+1^2, \end{array}$$

se observe que para representar a 7 se necesitan cuatro cuadrados, por lo que una respuesta parcial a la pregunta es $n\geq 4$. Sobra decir que existe la posibilidad de que algún entero requiera más de cuatro cuadrados. Un famoso teorema de Lagrange, demostrado en 1770, afirma que cuatro cuadrados son suficientes; es decir, todo entero positivo se puede representar como suma de cuatro cuadrados, alguno de los cuales puede ser $0=0^2$.

Para comenzar con temas más sencillos, primero se presentan condiciones necesarias y suficientes para que un entero positivo sea representable como suma de dos cuadrados. El problema se puede reducir a los números primos.

LEMA 8.4.1

Si m y n son sumas de dos cuadrados, entonces también lo es su producto mn.

Demostración: Si $m = a^2 + b^2$ y $n = c^2 + d^2$ para enteros a, b, c, d, entonces

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Q.e.d.

Es obvio que no todo primo puede ser escrito como suma de dos cuadrados, por ejemplo, $3 = a^2 + b^2$ no tiene solución en enteros a y b.

TEOREMA 8.4.1

Ningún número primo p de la forma $4k + 3$ es suma de dos cuadrados.

Demostración: Se conoce que todo entero a cumple que $a^2 \equiv 0,$ o $1(mod\ 4)$. Entonces $a^2 + b^2 \equiv 0, 1,$ o $2(mod\ 4)$. Como $p \equiv 3(mod\ 4)$, la ecuación $p = a^2 + b^2$ no tiene solución. **Q.e.d.**

Por otra parte, todo primo congruente a 1 módulo 4 es suma de dos cuadrados. La demostración requiere de un teorema sobre congruencias debido al matemático noruego Axel Thue. Por su parte, éste se apoya en el famoso "principio del palomar" de Dirichlet.

Principio del palomar

Si se ordenan n objetos en m cajas (o palomares) y si $n > m$, entonces alguna caja contiene al menos 2 objetos.

En términos más matemáticos, este simple principio afirma que si un conjunto de n elementos es la unión de m subconjuntos y si $n > m$, entonces algún subconjunto tiene más de un elemento.

LEMA 8.4.2 ***Thue***

Sea p primo y $(a, p) = 1$. Entonces la congruencia

$$ax \equiv y(mod\ p)$$

admite solución x_0, y_0, donde

$$0 < |x_0| < \sqrt{p}, \qquad 0 < |y_0| < \sqrt{p}.$$

Demostración: Sea $k = [\sqrt{p}] + 1$ y consideremos el conjunto de enteros

$$S = \{ax - y;\ 0 \leq x \leq k-1,\ 0 \leq y \leq k-1\}.$$

Como $ax - y$ toma $k^2 > p$ valores posibles, el principio del palomar garantiza que al menos dos miembros de S tienen que ser congruentes módulo p. Sean ellos $ax_1 - y_1$ y $ax_2 - y_2$, donde $x_1 \neq x_2$ y $y_1 \neq y_2$. Entonces se puede escribir

$$a(x_1 - x_2) \equiv y_1 - y_2 (mod\ p).$$

Haciendo $x_0 = x_1 - x_2$ y $y_0 = y_1 - y_2$, se tiene que x_0 y y_0 son una solución de la congruencia $ax \equiv y (mod\ p)$. Si alguno de ellos fuese cero, se puede usar el hecho de que $(a, p) = 1$ para comprobar que el otro también tiene que ser cero, contrario a lo asumido. Luego, $0 < |x_0| \leq k-1 < \sqrt{p}$ y $0 < |y_0| \leq k-1 < \sqrt{p}$.**Q.e.d.**

Ya estamos listos para deducir el famoso teorema de Fermat de que todo primo de la forma $4k + 1$ puede ser expresado como suma de dos cuadrados. En términos de prioridad, Girard recoconoció este hecho 7 años antes y el resultado se refiere en ocasiones como teorema de Girard. Fermat comunicó el resultado en una carta a Mersenne, fechada el 25 de diciembre de 1640, y decía que poseía una prueba irrefutable. Sin embargo, la primera prueba conocida y publicada se debe a Euler en 1754, quien tuvo éxito además al afirmar que la representación es única.

TEOREMA 8.4.2 ***Fermat***

Un número primo impar p se puede representar como suma de dos cuadrados si y sólo si $p \equiv 1 (mod\ 4)$.

Demostración: (Necesidad:) Supongamos que p puede ser escrito como suma de dos cuadrados, $p = a^2 + b^2$. Como p primo, se tiene que $p \nmid a$ y $p \nmid b$. (Si $p|a$, entonces $p|b^2$, de donde $p|b$, lo que conduce a la contradicción de que $p^2|p$.) Luego, por la teoría de congruencias lineales, existe un entero c tal que $bc \equiv 1 (mod\ p)$. Módulo p, la relación $(ac)^2 + (bc)^2 = (pc)^2$ se convierte en

$$(ac)^2 \equiv -1 (mod\ p),$$

por lo que -1 es residuo cuadrático de p. Pero del capítulo 6 se conoce que $\left(\frac{-1}{p}\right) = 1$ sólo cuando $p \equiv 1 (mod\ 4)$.

(Suficiencia:) Sea $p \equiv 1 (mod\ 4)$. Como -1 es residuo cuadrático de p, existe un entero tal que $a^2 \equiv -1 (mod\ p)$. De hecho, $a = \left[\frac{p-1}{2}\right]!$ es uno de esos enteros. Ahora, $(a, p) = 1$, de modo que la congruencia

$$ax \equiv y (mod\ p)$$

admite solución x_0, y_0, para la cual se cumple el lema de Thue. Como resultado es

$$-x_0^2 \equiv a^2x_0^2 \equiv (ax_0)^2 \equiv y_0^2 (mod\ p) \quad \text{o} \quad x_0^2 + y_0^2 \equiv 0 (mod\ p).$$

Entonces

$$x_0^2 + y_0^2 = kp$$

para cierto entero $k \geq 1$. Como $0 < |x_0| < \sqrt{p}$ y $0 < |y_0| < \sqrt{p}$, se tiene $0 < -x_0^2 + y_0^2 < 2p$, lo que implica que $k = 1$. Luego, $x_0^2 + y_0^2 = p$, lo que demuestra al teorema. **Q.e.d.**

Al considerar la igualdad de a^2 y $(-a)^2$, se obtiene el corolario siguiente.

Corolario 8.4.1

Todo primo p de la forma $4k + 1$ puede ser representado de modo único (excepto quizás por el orden de los sumandos) como suma de dos cuadrados.

Demostración: Supongamos que

$$p = a^2 + b^2 = c^2 + d^2,$$

donde a, b, c, d son enteros positivos. Entonces

$$a^2d^2 - b^2c^2 \equiv p(d^2 - b^2) \equiv 0 (mod\ p),$$

por lo que $ad \equiv bc (mod\ p)$ o $ad \equiv -bc (mod\ p)$. Como a, b, c, d son menores que 4, esas relaciones implican que $ad - bc = 0$ o $ad + bc = p$. Si se cumple la segunda, entonces $ac = bd$, pues

$$\begin{aligned} p^2 &= (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 \\ &= p^2 + (ac - bd)^2, \end{aligned}$$

de donde $ac - bd = 0$. De aquí que $ad = bc$ o $ac = bd$. Supongamos, por ejemplo, que $ad = bc$. Entonces $a|bc$ con $(a, b) = 1$, lo que obliga a que $a|c$, es decir, $c = ka$. La condición $ad = bc = b(ka)$ reduce a $d = bk$. Pero

$$p = c^2 + d^2 = k^2(a^2 + b^2)$$

implica que $k = 1$. En ese caso es $a = c$ y $b = d$. Con un argumento similar, la condición $ac = bd$ implica que $a = d$ y $4b = c$. Lo importante es que en cualquier caso

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

de donde se deduce la unicidad. **Q.e.d.**

Sigamos los pasos del teorema anterior, usando el primo $p = 13$. Una selección para el entero a es $6! = 720$. Una solución de la congruencia $720x \equiv y(mod\ 13)$, o mejor,

$$5x \equiv y(mod\ 13)$$

se obtiene al considerar el conjunto

$$S = \{5x - y;\ 0 \leq x, y < 4\}.$$

Los elementos de S son precisamente

$$\begin{array}{cccc} 5(0)-0=0, & 5(1)-0=5, & 5(2)-0=10, & 5(3)-0=15, \\ 5(0)-1=-1, & 5(1)-1=4, & 5(2)-1=9, & 5(3)-1=14, \\ 5(0)-2=-2, & 5(1)-2=3, & 5(2)-2=8, & 5(3)-2=13, \\ 5(0)-3=-3, & 5(1)-3=2, & 5(2)-3=7, & 5(3)-3=12, \end{array}$$

los cuales, módulo 13 son

$$\begin{array}{cccc} 0, & 5, & 10, & 2, \\ 12, & 4, & 9, & 1, \\ 11, & 3, & 8, & 0, \\ 10, & 2, & 7, & 12. \end{array}$$

Entre varias posibilidades de parejas de congruentes se tiene

$$5 \cdot 1 - 3 \equiv 2 \equiv 5 \cdot 3 - 0(mod 13) \ \text{ o } \ 5(1-3) \equiv 3(mod 13).$$

Luego, se puede elegir $x_0 = -2$ y $y_0 = 3$ para obtener

$$13 = x_0^2 + y_0^2 = 2^2 + 3^2.$$

Nota: Algunos autores afirman que todo primo $p \equiv 1(mod\ 4)$ puede ser escrito como suma de dos cuadrados de ocho maneras. Por ejemplo, para $p = 13$ se tiene

$$\begin{array}{rcl} 13 & = & 2^2 + 3^2 = (-2)2^2 + 3^2 = 2^2 + (-3)^2 = (-2)^2 + (-3)^2 \\ & = & 3^2 + 2^2 = 3^2 + (-2)2^2 = (-3)^2 + 2^2 = (-3)^2 + (-2)^2. \end{array}$$

Como cada representación se obtiene a partir de otra cambiando el signo o el orden, se puede considerar que son una "en esencia". Luego, desde nuestro punto de vista, 13 tiene una representación única como suma de dos cuadrados.

Hemos visto que todo primo $p \equiv 1(mod\ 4)$ puede ser escrito como suma de dos cuadrados. pero otros enteros disfrutan también de esa propiedad, por ejemplo,

$$10 = 1^2 + 3^2.$$

El siguiente paso es entonces explicitar aquellos enteros positivos que pueden ser escritos como suma de dos cuadrados.

Teorema 8.4.3

Sea el entero positivo n escrito en la forma $n = N^2m$, donde m es libre de cuadrados. Entonces n puede ser representado como suma de dos cuadrados si y sólo si m no contiene ningún factor primo de la forma $4k + 3$.

Demostración: (Suficiencia:) Supongamos que m no contiene ningún factor primo de la forma $4k + 3$. Si $m = 1$, entonces $n = N^2 + 0^2$ y se cumple la proposición. En el caso $m > 1$, sea $m = p_1p_2 \cdots p_r$ la factorización de m en un producto de números primos diferentes. Cada uno de esos primos p_i es igual a 2 o de la forma $4k + 1$, por lo que puede ser escrito como la suma de dos cuadrados. Pero la identidad

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

muestra que el producto de dos (y, por inducción, de cualquier cantidad finita) de números enteros que son sumas de dos cuadrados, es también representable de ese modo. Luego, existen enteros x, y tales que $m = x^2 + y^2$. Culminamos con la suma de dos cuadrados

$$n = N^2m = N^2(x^2 + y^2) = (Nx)^2 + (Ny)^2.$$

(Necesidad:) Supongamos que n es suma de dos cuadrados

$$n = a^2 + b^2 = N^2m,$$

y sea p un divisor primo cualquiera de m. Sin perder generalidad, podemos asumir que $m > 1$. Si $d = (a, b)$, se tiene $a = rd$, $b = sd$ con $(r, s) = 1$. Entonces

$$d^2(r^2 + s^2) = N^2m,$$

y por tanto, al ser m libre de cuadrados, se tiene que $d^2|N^2$. Pero entonces es

$$r^2 + s^2 = \frac{N^2}{d^2}m = tp,$$

para cierto entero t, de donde

$$r^2 + s^2 \equiv 0(mod\ p).$$

Ahora, la condición $(r, s) = 1$ implica que r o s (digamos r) es primo relativo con p. Sea r' que satisface la congruencia

$$rr' \equiv 1(mod\ p).$$

Si la ecuación $r^2 + s^2 \equiv 0(mod\ p)$ se multiplica por $(r')^2$, se obtiene

$$(sr')^2 + 1 \equiv 0(mod\ p),$$

o dicho de otro modo, $\left(\frac{-1}{p}\right) = 1$. Como -1 es residuo cuadrático de p, entonces $p \equiv 1(mod\ 4)$. Luego, ningún primo de la forma $4k + 3$ divide a m. **Q.e.d.**

COROLARIO 8.4.2

Un entero positivo n puede ser representado como suma de dos cuadrados si y sólo si cada uno de sus factores primos de la forma $4k+3$ aparece elevado a una potencia par.

EJEMPLO: El entero 459 no puede ser escrito como suma de dos cuadrados, pues $459 = 3^3 17$, con el primo 3 elevado a un exponente impar. Por otra parte, $153 = 3^2 17$ admite la representación

$$153 = 3^2(4^2 + 1^2) = 12^2 + 3^2.$$

Algo más complicado es el ejemplo $n = 5 \cdot 7^2 \cdot 13 \cdot 17$. En este caso es

$$n = 7^2 \cdot 5 \cdot 13 \cdot 17 = 7^2(2^2 + 1^2)(3^2 + 2^2)(4^2 + 1^2).$$

Aplicando la identidad mencionada en la demostración del teorema, se tiene

$$\begin{aligned}(3^2 + 2^2)(4^2 + 1^2) &= (12 + 2)^2 + (3 - 8)^2 = 14^2 - 5^2\\ (2^2 + 1^2)(14^2 + 5^2) &= (28 + 5)^2 + (10 - 14)^2 = 33^2 - 4^2.\end{aligned}$$

Finalmente, al combinarlas es

$$n = 7^2(33^2 + 4^2) = 231^2 + 28^2.$$

Existen ciertos enteros positivos (obviamente no primos de la forma $4k + 1$) que pueden ser representados de más de un modo como suma de dos cuadrados. El menor es

$$25 = 4^2 + 3^2 = 5^2 + 0^2.$$

Si $a \equiv b (mod\ 2)$, entonces la relación

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

permite crear toda una variedad de ejemplos. Por ejemplo, para $n = 153$ se tiene

$$153 = 17 \cdot 9 = \left(\frac{17+9}{2}\right)^2 - \left(\frac{17-9}{2}\right)^2 = 13^2 + 4^2,$$

y

$$153 = 51 \cdot 3 = \left(\frac{51+3}{2}\right)^2 - \left(\frac{51-3}{2}\right)^2 = 27^2 + 24^2.$$

Así se obtienen las dos representaciones diferentes

$$13^2 + 4^2 = 27^2 + 24^2 = 135.$$

En este punto, surge por sí misma una pregunta natural ¿qué enteros positivos admiten representación como diferencia de dos cuadrados? La respuesta aparece a continuación.

TEOREMA 8.4.4

Un entero positivo n puede ser representado como diferencia de dos cuadrados si y sólo si n no es de la forma $4k+2$.

Demostración: (Necesidad) Como $a^2 \equiv 0$ o $1(mod\ 4)$ para todo entero a, se cumple que $a^2 - b^2 \equiv 0, 1$ o $3(mod\ 4)$. Luego, si $n \equiv 2(mod\ 4)$, no puede ser $n = a^2 - b^2$ para cualquier selección de a y b.

(Suficiencia) Supongamos ahora que n no es de la forma $4k+2$, es decir, $n \equiv 0, 1$ o $3(mod\ 4)$. Si $n \equiv 1$ o $3(mod\ 4)$, entonces $n+1$ y $n-1$ son ambos pares, por lo que n puede ser escrito como diferencia de cuadrados en la forma

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

Si $n \equiv 0(mod\ 4)$, entonces

$$n = \left(\frac{n}{4}+1\right)^2 - \left(\frac{n}{4}-1\right)^2,$$

quedando así demostrado el teorema. **Q.e.d.**

COROLARIO 8.4.3

Todo primo impar es la diferencia de dos cuadrados sucesivos.

Ejemplos de éste último corolario son

$$11 = 6^2 - 5^2, \quad 17 = 9^2 - 8^2, \quad 29 = 15^2 - 14^2.$$

Otro punto que conviene mencionar es que la representación de un primo dado como diferencia de dos cuadrados es única. Para comprobarlo, supongamos que

$$p = a^2 - b^2 = (a-b)(a+b),$$

donde $a > b > 0$. Como los únicos factores de p son 1 y p, tiene que ser

$$a - b = 1 \qquad \text{y} \qquad a + b = p,$$

de donde se deduce que

$$a = \frac{p+1}{2} \qquad \text{y} \qquad b = \frac{p-1}{2}.$$

Luego, todo primo impar puede ser escrito de modo único como diferencia de dos cuadrados, a saber,

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

La situación es diferente al pasar de primos a enteros arbitrarios. Supongamos que n es un entero positivo que no es primo, ni de la forma $4k+2$. Partiendo de un divisor d de n, hacemos $d' = \frac{n}{d}$ (se puede asumir sin perder generalidad que $d > d'$). Ahora, si d y d' tienen igual paridad, entonces

$$\frac{d+d'}{2} \qquad \text{y} \qquad \frac{d-d'}{2}$$

son enteros. Más aún, se puede escribir

$$n = dd' = \left(\frac{d+d'}{2}\right)^2 - \left(\frac{d-d'}{2}\right)^2.$$

Como ejemplo, para el entero $n = 24$ es

$$24 = 12 \cdot 2 = \left(\frac{12+2}{2}\right)^2 - \left(\frac{12-2}{2}\right)^2 = 7^2 - 5^2$$

y

$$24 = 6 \cdot 4 = \left(\frac{6+4}{2}\right)^2 - \left(\frac{6-4}{2}\right)^2 = 5^2 - 1^2,$$

de modo que se tienen dos representaciones de 24 como diferencia de dos cuadrados.

8.4.2. Ejercicios

1. Represente cada uno de los números primos 113, 229 y 373 como suma de dos cuadrados.

2. *a*) Se ha conjeturado que existen infinitos primos p tales que $p = n^2 + (n+1)^2$ para cierto entero positivo n; por ejemplo, $5 = 1^2 + 2^2$ y $13 = 2^2 + 3^2$. Halle cinco más de esos primos.

   b) Otra conjetura es que que existen infinitos primos de la forma $p = 2^2 + p_1^2$, donde p_1 es primo. Halle cinco de esos primos.

3. Demuestre las siguientes proposiciones:

   a) Todo entero de la forma 2^n, donde $n = 1, 2, 3, \ldots$, es suma de dos cuadrados.

   b) Si $n \equiv 3$ o $6 (mod\ 9)$, entonces n no puede ser representado como suma de dos cuadrados.

   c) Si n es la suma de dos números triangulares, entonces $4n+1$ es suma de dos cuadrados.

   d) Todo número de Fermat $F_n = 2^{2^n} + 1$ para $n \geq 1$ es suma de dos cuadrados.

   e) Todo número perfecto impar (si existiera) es la suma de dos cuadrados. (Sugerencia: vea el corolario 8.1.1 del epígrafe 8.1 .)

4. Demuestre que el número primo p es suma de dos cuadrados si y sólo si la congruencia $x^2 + 1 \equiv 0(mod\ p)$ admite solución.

5. *a*) Demuestre que un entero positivo n es suma de dos cuadrados. si y sólo si $n = 2^m a^2 b$, donde $m \geq 0$, a es impar y todo divisor primo de b es de la forma $4k + 1$.

   b) Escriba como suma de dos cuadrados los enteros

$$3185 = 5 \cdot 7^2 13, \quad 39690 = 2 \cdot 3^4 5 \cdot 7^2 \quad \text{y} \quad 62920 = 2^3 5 \cdot 11^2 \cdot 13.$$

6. Encuentre un entero positivo que tenga al menos tres representaciones diferentes como suma de dos cuadrados, sin tener en cuenta el signo o el orden de los sumandos. (Sugerencia: seleccione un entero que tenga tres factores primos diferentes, todos de la forma $4k + 1$.)

7. Si el entero positivo n no es suma de dos cuadrados de enteros, demuestre que n no puede ser representado como suma de dos cuadrados de números racionales. (Sugerencia: Se ha demostrado existe un primo $p \equiv 3(mod\ 4)$ y un entero impar k tales que $p^k | n$ mientras que $p^{k+1} \nmid n$; si

$$n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2,$$

   entonces p aparece elevado a un potencia impar en el miembro izquierdo de la ecuación

$$n(bd)^2 = a^2 + c^2,$$

   pero no en el miembro derecho.)

8. Demuestre que el entero positivo n tiene tantas representaciones como suma de dos cuadrados como el entero $2n$. (Sugerencia: partiendo de una representación de n como suma de dos cuadrados, obtenga una similar para $2n$ y viceversa.)

9. *a*) Si n es un número triangular, demuestre que los tres enteros sucesivos $8n^2$, $8n^2 + 1$, $8n^2 + 2$ pueden ser escritos como suma de dos cuadrados.

   b) Demuestre que de cualesquiera cuatro enteros consecutivos, al menos uno no es representable como suma de dos cuadrados.

10. Demuestre que:

    a) si un número primo es suma de dos o cuatro cuadrados de primos diferentes, entonces uno de esos primos tiene que ser igual a 2.

    b) si un número primo es suma de cuadrados de tres primos diferentes, entonces uno de esos primos tiene que ser igual a 3.

11. *a*) Sea p primo impar. Si $p|a^2+b^2$ con $(a,b)=1$, demuestre que se cumple $p \equiv 1(mod\ 4)$. (Sugerencia: eleve la congruencia $a^2 \equiv -b^2(mod\ p)$ a la potencia $\frac{p-1}{2}$ y apliqe el teorema de Fermat para concluir que $(-1)^{\frac{p-1}{2}} = 1$.)

    b) Use el inciso a) para demostrar que todo divisor positivo de una suma de dos cuadrados primos relativos es a su vez suma de dos cuadrados.

12. Compruebe que todo primo p de la forma $8k+1$ ó $8k+3$ puede ser escrito como $p = a^2+2b^2$ para ciertos enteros a, b. (Sugerencia: repita la demostración del teorema 8.4.2.)

13. Demuestre que:

    a) Un entero positivo es representable como diferencia de dos cuadrados si y sólo si es producto de dos factores de igual paridad.

    b) Un entero positivo es representable como diferencia de dos cuadrados si y sólo si es divisible por 4.

14. Verifique que 45 es el menor entero positivo que admite tres representaciones diferentes como diferencia de dos cuadrados. (Sugerencia: vea el inciso a) del problema anterior.)

15. Para todo $n > 0$, demuestre que existe un entero positivo que puede ser expresado en n modos diferentes como diferencia de dos cuadrados. (Sugerencia: note que
$$2^{2n+1} = \left(2^{2n-k} + 2^{k-1}\right)^2 - \left(2^{2n-k} - 2^{k-1}\right)^2$$
para $k = 1, 2, \ldots, n$.)

16. Demuestre que todo primo $p \equiv 1(mod\ 4)$ divide a la suma de dos cuadrados primos relativos, donde cada cuadrado excede a 3. (Sugerencia: dada una raíz primitiva impar r de p, es $r^k \equiv 2(mod\ p)$, de donde se deduce que $r^{2[k+(p-1)/4]} \equiv -4(mod\ p)$.)

17. Demuestre que la ecuación $n^2 + (n+1)^2 = m^3$ no tiene solución en $\mathbb{Z}_+$.

18. El especialista en Teoría de Números inglés G. H. Hardy relata la siguiente historia sobre su joven protegido Ramanujan:

    > "*Recuerdo haber ido a visitarlo cuando estaba en cama enfermo en Putney. Yo había viajado en el taxi con el número* 1729*, y le comenté que el número me parecía más bien tonto y que esperaba que no fuera una profecía desfavorable. 'No,'respondió el, 'se trata de es un número muy interesante, pues es el menor número expresable como suma de dos cubos de dos maneras diferentes.*"

    Compruebe la afirmación de Ramanujan.

8.4.3. Suma de más de dos cuadrados

Mientras que no todo entero puede ser escrito como suma de dos cuadrados ¿qué decir acerca de representarlos como suma de tres cuadrados? Agregando un nuevo cuadrado, es razonable esperar que existan menos excepciones. Por ejemplo, 14, 33 y 67 no son suma de dos cuadrados, pero

$$\begin{aligned} 14 &= 3^2 + 2^2 + 1^2 \\ 33 &= 5^2 + 2^2 + 2^2 \\ 67 &= 7^2 + 3^2 + 3^2. \end{aligned}$$

Es posible encontrar enteros que no son expresables como suma de tres cuadrados.

Teorema 8.4.5

Ningún entero de la forma $4^n(8m + 7)$ puede ser representado como suma de tres cuadrados.

Demostración: Veamos primeramente que $8m + 7$ no es expresable como suma de tres cuadrados. Ya sabemos que para todo entero a es $a^2 \equiv 0, 1 \quad \text{o} \quad 4(mod\ 8)$. Entonces $a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5 \quad \text{o} \quad 6(mod\ 8)$ para cualquier selección de a, b, c. Como $8m + 7 \equiv 7(mod\ 8)$, la ecuación $a^2 + b^2 + c^2 = 8m + 7$ no tiene solución.

Ahora supongamos que $4^n(8m + 7)$, donde $n \geq 1$, puede ser escrito como

$$4^n(8m + 7) = a^2 + b^2 + c^2.$$

Entonces cada uno de los enteros a, b, c tiene que ser par. Haciendo $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, y se obtiene

$$4^{n-1}(8m + 7) = a_1^2 + b_1^2 + c_1^2.$$

Si $n - 1 \geq 1$ se repite el proceso hasta llegar a que $8m + 7$ puede ser representado como suma de tres cuadrados, lo cual es una contradicción con lo demostrado en el párrafo anterior. **Q.e.d.**

Se puede demotrar que la condición de este teorema es también suficiente para que un número entero sea expresable como suma de tres cuadrados, pero la demostración es muy compleja para incluirla aquí. Parte del problema es que, a no ser en el caso de dos (o cuatro) cuadrados, no existe ninguna identidad algebraica que exprese el producto de sumas de tres cuadrados en esa misma forma.

Veamos algunas notas históricas. Diofanto conjeturó que ningún número de la forma $8m + 7$ es suma de tres cuadrados, un hecho fácilmente verificado por Descartes en 1638. Es justo dar el crédito a Fermat por ser el primero en plantear el criterio completo de que un número puede ser escrito como suma de tres cuadrados si y sólo si no es de la forma $4^n(8m + 7)$, donde m y n son enteros no negativos. Esto fue

demostrado de modo complicado por Legendre en 1798 y luego de manera más clara (y no por ello más sencilla) por Gauss en 1801.

Como ya se ha indicado, existen enteros que no son representables como suma de tres cuadrados (por ejemplo, 5 y 7). Ello cambia dramáticamente cuando se pasa a cuatro cuadrados ¡en ese caso, no hay excepciones !

8.4.4. Cuatro cuadrados y su autor

Tras la muerte de Descartes, Pascal y Fermat, no apareció ningún otro matemático francés de estatura comparable por más de un siglo. Mientras tanto, en Inglaterra y Suecia avanzaban los estudios matemáticos. Hacia finales del siglo XVIII, París se convierte nuevamente en el centro de los estudios matemáticos, cuando Lagrange, Laplace y Legendre traen nueva gloria a Francia.

Italiano de nacimiento, alemán por adopción y francés por elección, Joseph Louis Lagrange (1736-1813) fue, según algunos historiadores, el segundo más famoso matemático del siglo XVIII después de Euler. Cuando entró a la Universidad de Turin, su gran interés era la Física, pero tras leer un tratado de Halley sobre los méritos del cálculo newtoniano, le excitó la nueva Matemática que estaba transformando la mecánica celeste. Se dedicó con tanto ímpetu a los estudios matemáticos, que fue nombrado profesor de Geometría de la Escuela Real de Artillería de Turin a la edad de 18 años. No demoró Lagrange en ser incluido entre los competidores por el premio bienal de la Academia Francesa de Ciencias y entre 1764 y 1788 ganó cinco de los premios por sus aplicaciones de la Matemática a problemas de la Astronomía.

Durante varias años, Lagrange fue el director de la sección de Matemática de la Academia de Berlín, y produjo una importante obra, cuyo punto culminante fue su tratado monumental, la "Mécanique Analitique" (publicado en 1788 en cuatro volúmenes). En 1787 decidió aceptar la invitación de Louis XVI para asentarse en Paris, donde tomó la cuidadanía francesa. Tras la abolición con la revolución francesa en 1793 de todas las antiguas universidades francesas (la Academia de Ciencias también había sido suprimida), los revolucionarios crearon dos nuevas escuelas con los humildes títulos de Ecole Normale y Ecole Polytechnique, y Lagrange fue invitado a impartir las conferencias de Análisis. Sus notas de las conferencia de Cálculo Diferencial constituyeron la base de otro clásico de la Matemática, la "Théorie des Fonctions Analitique" (1797).

A pesar de que las investigaciones de Lagrange cubrieron un espectro extraordinariamente amplio, el poseía, como Diofanto y Fermat, un talento especial para la Teoría de Números. Su obra en esa área incluye la primera demostración del Teorema de Wilson; la investigación de las condiciones bajo las cuales ± 2 y ± 5 son residuos cuadráticos de un primo impar; encontró todas las soluciones enteras de la ecuación $x^2 - ay^2 = 1$; así como la solución de varios problemas propuestos por

Fermat respecto a las representaciones particulares de ciertos primos.

Este epígrafe se centra en el descubrimiento que dio gran renombre a Lagrange en la Teoría de Números, la demostración de que todo entero positivo puede ser expresado como suma de cuatro cuadrados.

La primera referencia explícita al hecho de que todo entero es suma de cuatro cuadrados fue realizada por Bachet (en 1621), quien comprobó su conjetura para todos los enteros hasta 325. Quince años después, Fermat anunció tener una demostración usando su método favorito del descenso infinito, pero, como era usual, no dio detalles. Ambos, Bachet y Fermat, sentían que Diofanto debía haber conocido el resultado, pero Diofanto nunca hizo mención alguna al caso de los cuatro cuadrados.

Una medida de la dificultad del problema es el hecho de que Euler, a pesar de sus inteligentes resultados, trabajó en el tema sin éxito por más de 40 años. Sin embargo, su contribución a la solución eventual fue sustancial; Euler descubrió la identidad fundamental que permite expresar el producto de sumas de cuatro cuadrados como una suma de ese tipo, así como el resultado crucial de que la congruencia $x^2 + y^2 + 1 \equiv 0(mod\ p)$ tiene solución para todo primo p. La demostración completa de la conjetura de los cuatro cuadrados fue publicada por Lagrange en 1772, quien reconoció su deuda a las ideas de Euler. Al año siguiente Euler publicó una demostración mucho más simple, cuya versión es la que se presenta aquí en sus rasgos esenciales.

Resulta conveniente establecer dos lemas preparatorios, para no tener que interrumpir la demostración en su parte fundamental. El primero contiene la identidad que permite reducir el estudio al caso de los números primos.

LEMA 8.4.3 ***Euler***

Si los enteros m y n son suma de cuatro cuadrados, entonces mn también lo es.

Demostración: Si

$$m = a_1^2 + a_2^2 + a_3^2 + a_4^2 \qquad \text{y} \qquad n = b_1^2 + b_2^2 + b_3^2 + b_4^2,$$

para enteros a_i, b_i, entonces

$$\begin{aligned} mn &= (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ &= (a_l b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4)^2 + (a_1 b_2 - a_2 b_1 + a_3 b_4 - a_4 b_3)^2 \\ &\quad + (a_1 b_3 - a_2 b_4 - a_3 b_1 + a_4 b_2)^2 + (a_1 b_4 + a_2 b - 3 - a_3 b_2 - a_4 b_1)^2. \end{aligned}$$

Esta identidad se comprueba por fuerza bruta, multiplicando y comparando términos, lo cual resulta demasiado extenso para esta página. **Q.e.d.**

Otro resultado básico es el siguiente.

LEMA 8.4.4

Si p es primo impar, entonces la congruencia $x^2 + y^2 + 1 \equiv 0(mod\ p)$ tiene una solución x_0, y_0, donde $0 \leq x_0, y_0 \leq \frac{p-1}{2}$.

Demostración: La esencia de la demostración consiste en considerar los siguientes conjuntos:

$$\begin{aligned} S_1 &= \left\{1 + 0^2, 1 + 1^2, 1 + 2^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2\right\}, \\ S_2 &= \left\{-0^2, -1^2, -2^2, \ldots, -\left(\frac{p-1}{2}\right)^2\right\}. \end{aligned}$$

Evidentemente los elementos del conjunto S_1 son incongruentes módulo p, pues si $1 + x_1^2 \equiv 1 + x_2^2(mod\ p)$, entonces $x_1 \equiv x_2(mod\ p)$ o $x_1 \equiv -x_2(mod\ p)$. Pero la última congruencia es imposible, dado que $0 < x_1 + x_2 < p$ (excepto $x_1 = x_2 = 0$), por lo que $x_1 \equiv x_2(mod\ p)$, lo que implica $x_1 = x_2$. Del mismo modo se comprueba que los elementos del conjunto S_2 son incongruentes módulo p.

Juntos S_1 y S_2 contienen $2[1 + \frac{1}{2}(p-1)] = p + 1$ enteros. Por el principio del palomar, cierto entero de S_1 tiene que ser congruente módulo p a cierto entero de S_2. Es decir, existen enteros x_0, y_0 tales que

$$1 + x_0^2 \equiv -y_0^2(mod\ p),$$

donde $0 \leq x_0, y_0 \leq \frac{p-1}{2}$. **Q.e.d.**

COROLARIO 8.4.4

Dado un número primo impar p, existe un entero $k < p$ tal que kp es la suma de cuatro cuadrados.

Demostración: De acuerdo al teorema, se pueden encontrar enteros x_0, y_0 con

$$0 \leq x_0, y_0 < \frac{p}{2}$$

y tales que

$$1 + x_0^2 + y_0^2 = kp,$$

para cierto k. Las restriciones para x_0, y_0 implican que $k < p$. **Q.e.d.**

Veamos un ejemplo. Para $p = 17$, los conjuntos S_1 y S_2 son

$$\begin{aligned} S_1 &= \{1, 2, 5, 10, 17, 26, 37, 50, 65\}, \\ S_2 &= \{0, -1, -4, -9, -16, -25, -36, -49, -64\}. \end{aligned}$$

y módulo 17 son

$$\begin{aligned} S_1 &= \{1, 2, 5, 10, 0, 9, 3, 16, 14\}, \\ S_2 &= \{0, 16, 13, 8, 1, 9, 15, 2, 4\}. \end{aligned}$$

El lema anterior indica que un elemento $1 + x^2$ de S_1 es congruente módulo p a un y^2 de S_2. Entre varias posibilidades se tiene

$$1 + 5^2 \equiv 9 \equiv -5^2 (mod\ 17) \quad \text{o} \quad 1 + 5^2 + 5^2 \equiv 0 (mod\ 17).$$

Entonces

$$3 \cdot 17 = 1^2 + 5^2 + 5^2 + 0^2$$

es un múltiplo de 17 escrito como suma de cuatro cuadrados.

Este lema es tan esencial para nuestro trabajo, que tiene también otra aproximación, esta vez en relación con la teoría de los residuos cuadráticos. Si $p \equiv 1 (mod\ 4)$, podemos seleccionar x_0 como solución de $x^2 \equiv -1 (mod\ p)$ (eso es posible por el corolario 4.3.1 del teorema 4.3.2 del capítulo 4) y $y_0 = 0$, para obtener

$$x_0^2 + y_0^2 + 1 \equiv 0 (mod\ p).$$

Luego, basta concentrarse en al caso $p \equiv 3 (mod\ 4)$. Sea a el menor no-residuo cuadrático positivo de p (observe que $a \geq 2$, pues 1 es residuo cuadrático). Entonces

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)(-1) = 1,$$

por lo que $-a$ es residuo cuadrático de p. Luego, la congruencia

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

admite solución x_0 con $0 < x_0 \leq \frac{p-1}{2}$. Como $a - 1$ es positivo y menor que a, tiene que ser residuo cuadrático de p. Entonces existe un entero y_0 con $0 < y_0 \leq \frac{p-1}{2}$ que cumple

$$y_0^2 \equiv a - 1 (mod\ p).$$

La conclusión es

$$x_0^2 + y_0^2 + 1 \equiv -a + (a - 1) + 1 \equiv 0 (mod\ p).$$

Con estos dos lemas entre nuestras herramientas, disponemos de la información necesaria para desarrollar la demostración esperada.

Teorema 8.4.6

Todo número primo p puede ser escrito como suma de cuatro cuadrados.

Demostración: El teorema es válido para $p = 2$, pues

$$2 = 1^2 + 1^2 + 0^2 + 0^2.$$

Luego, centraremos nuestra atención en los primos impares. Sea k el menor entero positivo tal que kp es suma de cuatro cuadrados, digamos

$$kp = x^2 + y^2 + z^2 + w^2.$$

Por el corolario anterior es $k < p$. Demostremos que $k = 1$, de modo que p es la suma de cuatro cuadrados.

Veamos primeramente que k es impar. Para ello, supongamos que k es par. Entonces x, y, x, w son todos pares, o todos impares, o dos son pares y dos impares. En todo caso podemos reordenarlos de modo que

$$x \equiv y(mod\ 2) \qquad \text{y} \qquad z \equiv w(mod\ 2).$$

Entonces

$$\frac{1}{2}(x-y), \quad \frac{1}{2}(x+y), \quad \frac{1}{2}(z-w), \quad \frac{1}{2}(z+w)$$

son enteros y

$$\frac{1}{2}(kp) = \left(\frac{1}{2}(x-y)\right)^2 + \left(\frac{1}{2}(x+y)\right)^2 + \left(\frac{1}{2}(z-w)\right)^2 + \left(\frac{1}{2}(z+w)\right)^2$$

es una representación de $\frac{k}{2}p$ como suma de cuatro cuadrados. Ello viola la naturaleza minimal de k, llegando así a una contradicción.

Asumamos ahora que $k \neq 1$. Entonces, como k es impar, es $k \geq 3$. Así es posible encontrar enteros a, b, c, d tales que

$$a \equiv x(mod\ k), \quad b \equiv y(mod\ k), \quad c \equiv z(mod\ k), \quad d \equiv w(mod\ k)$$

y

$$|a| < \frac{k}{2}, \qquad |b| < \frac{k}{2}, \qquad |c| < \frac{k}{2}, \qquad |d| < \frac{k}{2}.$$

(Por ejemplo, para obtener a, halle el resto r de la división de x por k, haga $a = r$ o $a = r - k$ según sea $r < \frac{k}{2}$ ó $r > \frac{k}{2}$). Entonces

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0(mod\ k),$$

de donde

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

para cierto entero no negativo n. Por las restricciones para a, b, c, d es

$$0 \leq nk = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{k}{2}\right)^2 = k^2.$$

No puede ser $n = 0$, pues ello significaría que $a = b = c = d = 0$ y, en consecuencia k divide a cada uno de los enteros x, y, z, w. Entonces $k^2|kp$ o $k|p$, lo cual es imposible a causa de la desigualdad $1 < k < p$. La relación $nk < k^2$ también implica que $n < k$. En fin, $0 < n < k$. Combinando las piezas, se obtiene

$$\begin{aligned} k^2np &= (kp)(kn) = (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) \\ &= r^2 + s^2 + t^2 + u^2, \end{aligned}$$

donde

$$\begin{aligned} r &= xa + yb + zc + wd, \\ s &= xb - ya + zd - wc, \\ t &= xc - yd - za + wb, \\ u &= xd + yc - zb - wa. \end{aligned}$$

Observe que todos r, s, t, u son divisibles por k. En el caso de r, por ejemplo, es

$$r = xa + yb + zc + wd \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 (mod\ k).$$

De modo análogo es $s \equiv t \equiv u \equiv 0 (mod\ k)$. De ello se deduce la representación

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2,$$

donde $\frac{r}{k}$, $\frac{s}{k}$, $\frac{t}{k}$, $\frac{u}{k}$ son todos enteros. Como $0 < n < k$, se tiene una contradicción con la selección de k como el menor entero positivo para el que kp es suma de cuatro cuadrados. Entonces es $k = 1$, lo que culmina la demostración. **Q.e.d.**

Llegamos entonces a nuestro objetivo final, el resultado clásico de Lagrange.

TEOREMA 8.4.7 ***Lagrange***

Todo entero positivo puede ser escrito como suma de cuatro cuadrados, algunos de los cuales pueden ser cero.

Demostración: Obviamente es

$$1 = 1^2 + 0^2 + 0^2 + 0^2.$$

Sea $n > 1$ y sea $n = p_1 p_2 \cdots p_r$ la factorización de n en primos (no necesariamente distintos). Como cada p_i es suma de cuatro cuadrados, la identidad de Euler permite expresar el producto de dos primos como suma de cuatro cuadrados. Esto se extiende por inducción a cualquier cantidad finita de factores, de modo que aplicando la identidad r veces, se obtiene la representación deseada de n. **Q.e.d.**

EJEMPLO: Para escribir a $459 = 3^3 17$ como suma de cuatro cuadrados, se aplica la identidad de Euler como sigue:

$$\begin{aligned} 459 = 3^3 17 &= 3^2(1^2+1^2+1^2+0^2)(4^2+1^2+0^2+0^2) \\ &= 3^2\left[(4+1+0+0)^2+(1-4+0-0)^2\right. \\ &\quad \left.+(0-0-4+0)^2+(0+0-1-0)^2\right] \\ &= 3^2\left[5^2+3^2+4^2+1^2\right] \\ &= 15^2+9^2+12^2+3^2. \end{aligned}$$

Aunque los cuadrados han recibido toda nuestra atención, resulta importante mencionar que algunas ideas se relacionan con potencias mayores.

En su libro "Meditationes Algebraicae" (1770), Edward Waring afirmó que todo entero positivo es expresable como suma de de 9 cubos a lo sumo, suma de 19 potencias cuartas a lo sumo, y así sucesivamente. Esta afirmación se relaciona con la pregunta ¿puede ser expresado todo entero positivo como suma de no más de un número fijo $g(k)$ de k-ésimas potencias, donde $g(k)$ sólo depende de k y no del entero a ser representado? En otras palabras, dado k, un número $g(k)$ es tal que todo $n > 0$ puede ser representado de al menos una manera como

$$n = a_1^k + a_1^k + \ldots + a_{g(k)}^k,$$

donde los a_i so enteros no negativos, no necesariamente distintos. El problema resultante fue el punto de partida para una gran área de investigación de la teoría de números, que se ha hecho conocida como "**problema de Waring**". Parece algo dudoso que Waring haya desarrollado cálculos numéricos en favor de esa afirmación y no hay sombras de una prueba.

El teorema de Lagrange afirma que $g(2) = 4$. Excepto para los cuadrados, el primer caso de un problema de tipo Waring completamente demostrado se atribuye a Liouville (1859): todo entero positivo es suma de a lo sumo 53 potencias cuartas. Esa cota para $g(4)$ es algo grande y en los años siguientes se fue reduciendo progresivamente. La existencia de $g(k)$ para todo valor de k fue resuelta afirmativamente por Hilbert en 1909. Desafortunadamente, su demostración incluye una fuerte maquinaria (con integrales múltiples de orden 25) y no es construciva.

Una vez conocido que el problema de Waring admite solución, una pregunta natural es ¿cuán grande es $g(k)$? Existe mucha literatura que ataca esta parte del problema, pero el problema en sí permanece aún abierto. Un ejemplo que se debe a Dickson es que $g(3) = 9$, mientras que

$23 = 2^3+2^3+1^3+1^3+1^3+1^3+1^3+1^3+1^3$ y $239 = 4^3+4^3+4^3+3^3+3^3+3^3+1^3+1^3+1^3$

son los únicos enteros que requieren 9 cubos en su representación. Todo entero mayor que 239 es suma de a los sumo 8 cubos. En 1942 Linnik demostró que sólo una cantidad finita de enteros necesitan 8 cubos, pues a partir de cierto número bastan 7. Aún no se sabe si 6 cubos son también suficientes para representar una cantidad finita o infinita de enteros.

Otro problema que ha atraído considerablemente la atención es cuándo una potencia n-ésima puede ser expresada como suma de potencias n-ésimas para $n > 3$. El primer progreso fue realizado en 1911 con el descubrimiento de la menor solución en potencias cuartas

$$353^4 = 30^4 + 120^4 + 272^4 + 315^4.$$

En las potencias quintas la menor solución es

$$72^5 = 19^5 + 43^5 + 46^5 + 47^5 + 67^5.$$

Sin embargo, para potencias sextas o mayores no se conoce la solución aún.

Una pregunta relacionada es ¿puede una potencia n-ésima ser suma de menos de n potencias n-ésimas? Euler conjeturó que ellos es imposible, pero en 1968 Lander y Parkin lograron la representación

$$144^5 = 27^5 + 84^5 + 110^5 + 133^5.$$

A pesar de la extensa búsqueda computacional para potencias cuartas y sextas, este es el único contraejemplo conocido.

8.4.5. Ejercicios

1. Sin sumar los cuadrados, confirme las siguientes relaciones:

   a) $1^2 + 2^2 + 3^2 + \ldots + 23^2 + 24^2 = 70^2$.

   b) $18^2 + 19^2 + 20^2 + \ldots + 27^2 + 28^2 = 77^2$.

   c) $2^2 + 5^2 + 8^2 + \ldots + 23^2 + 26^2 = 48^2$.

   d) $6^2 + 12^2 + 18^2 + \ldots + 42^2 + 48^2 = 95^2 - 41^2$.

2. Regiomontanus propuso el problema de encontrar veinte cuadrados cuya suma sea un cuadrado mayor que 300 000. Halle dos soluciones. (Sugerencia: considere la identidad

$$\begin{aligned}(a_1^2 + a_2^2 + \ldots + a_n^2)^2 &= (a_1^2 + a_2^2 + \ldots + a_{n-1}^2 - a_n^2)^2 \\ &\quad +(2a_1a_n)^2 + (2a_2a_n)^2 + \ldots + (2a_{n-1}a_n)^2.\end{aligned}$$

3. Demuestre que $n^2 + (n+1)^2 + (n+2)^2 + \ldots + (n+k)^2$ no es un cuadrado si $1^2 + 2^2 + 3^2 + \ldots + k^2$ es no-residuo cuadrático de $k+1$.

4. Demuestre que la ecuación $a^2 + b^2 + c^2 + a + b + c = 1$ no tiene solución en los enteros. (Sugerencia: la ecuación dada es equivalente a la ecuación

$$(2a + 1)^2 + (2b + 1)^2 + (2c + 1)^2 = 7.)$$

5. Para un entero positivo n, demuestre que n o $2n$ es suma de tres cuadrados.

6. Un problema aún abierto es si existen infinitos primos p tales que para cierto $n > 0$ se cumple $p = n^2 + (n + 1)^2 + (n + 2)^2$. Halle tres de esos primos.

7. En nuestro estudio de $n = 459$ no se encontró ninguna representación como suma de dos cuadrados. Exprese 459 como suma de tres cuadrados.

8. Demuestre las siguientes proposiciones:

   a) Todo entero positivo impar es de la forma $a^2 + b^2 + 2c^2$, donde a, b, c son enteros. (Sugerencia: dado $n > 0$, $4n + 2$ puede ser escrito como $4n + 2 = x^2 + y^2 + z^2$ con x impar y y y z pares, entonces

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

   b) Todo entero positivo es de la forma $a^2+b^2+c^2$ ó $a^2+b^2+2c^2$, donde a, b, c son enteros. (Sugerencia: si $n > 0$ no puede ser escrito como $a^2 + b^2 + c^2$, entonces es de la forma $4^m(8k + 7)$; aplique el inciso a) al entero $8k + 7$.)

   c) Todo entero positivo es de la forma $a^2 + b^2 - c^2$, donde a, b, c son enteros. (Sugerencia: dado $n > 0$, seleccione a tal que $n - a^2$ es impar positivo y aplique el teorema 8.4.4.)

9. Demuestre las siguientes proposiciones:

   a) Ningún entero de la forma $9k + 4$ ó $9k + 5$ puede ser suma de tres o menos cubos. (Sugerencia: por el problema 10 de la sección 1 del capítulo IV es $a^3 \equiv 0, 1$ ó $8(mod\ 9)$ para todo entero a.)

   b) El único primo representable como suma de dos cubos es $p = 2$. (Sugerencia: use la identidad $a^3 + b^3 = (a + b)((a - b)^2 + ab)$.)

   c) Un primo p es diferencia de dos cubos si y sólo si p es de la forma $p = 3k(k + 1) + 1$.

10. Exprese cada uno de los primos $7, 19, 37, 61$ y 127 como diferencia de dos cubos.

11. Demuestre que todo entero positivo puede se representado como diferencia de tres o menos números triangulares. (Sugerencia: dado $n > 0$, exprese $8n + 3$ como suma de tres cuadrados impares y resuelva luego en n.)

12. Demuestre que existen infinitos primos p de la forma $p = a^2 + b^2 + c^2 + 1$, donde a, b, c son enteros. (Sugerencia: existen infinitos primos p de la forma $p = 8k + 7$; escriba
$$p - 1 = 8k + 6 = a^2 + b^2 + c^2$$
para ciertos a, b, c.)

13. Exprese los enteros
$$231 = 3 \cdot 7 \cdot 11, \qquad 391 = 17 \cdot 23, \qquad 2109 = 37 \cdot 57$$
como suma de cuatro cuadrados.

14. *a*) Demuestre que todo entero $n \geq 170$ es suma de cinco cuadrados, ninguno de los cuales es cero. (Sugerencia: escriba $n - 169 = a^2 + b^2 + c^2 + d^2$ para a, b, c, d enteros y considere los casos en que uno o más de a, b, c es cero.)

    b) Demuestre que todo múltiplo positivo de 8 es suma de ocho cuadrados impares. (Sugerencia: si $n = a^2 + b^2 + c^2 + d^2$, entonces $8n + 8$ es la suma de los cuadrados de $2a \pm 1$, $2b \pm 1$, $2c \pm 1$ y $2d \pm 1$.)

15. Del hecho de que $n^3 \equiv n (mod\ 6)$ deduzca que todo entero n puede ser representado como la suma de los cubos de cinco enteros, permitiendo cubos negativos. (Sugerencia: utilize la identidad
$$n^3 - 6k = n^3 - (k+1)^3 - (k-1)^3 + k^3 + k^3.$$

16. Demuestre que todo entero impar es la suma de cuatro cuadrados, dos de ellos consecutivos. (Sugerencia: para $n > 0$, $4n + 1$ es suma de tres cuadrados, siendo sólo uno impar; pero $4n + 1 = (2a)^2 + (2b)^2 + (2c + 1)^2$ implica que $2n + 1 = (a + b)^2 + (a - b)^2 + c^2 + (c + 1)^2$.)

17. Demuestre que existen infinitos números triangulares que son expresables como la suma de dos cubos y la diferencia de dos cubos. Muestre las representaciones de uno de esos números triangulares. (Sugerencia: en la identidad
$$\begin{aligned}(27k^6)^2 - 1 &= (9k^4 - 3k)^3 + (9k^3 - 1)^3 \\ &= (9k^4 + 3k)^3 - (9k^3 + 1)^3\end{aligned}$$
considere a k impar para obtener
$$(2n + 1)^2 - 1 = (2a)^3 + (2b)^3 = (2c)^3 - (2d)^3,$$
o lo que es equivalente $t_n = a^3 + b^3 = c^3 - d^3$.)

18. *a*) Si $n - 1$ y $n + 1$ son ambos primos, demuestre que el entero $2n^2 + 2$ puede ser representado como la suma de 2, 3, 4 y 5 cuadrados.

    b) Ilustre el resultado del inciso a) en los casos en que $n = 4, 6, 12$.

8.5. La sucesión de Fibonacci

8.5.1. La fama de Leonardo de Pisa

Leonardo de Pisa, Fibonacci, nació en 1180 en el seno de una familia de mercaderes italianos que por razones comerciales se trasladaron a Argelia. El padre le inició en los asuntos de negocios y le enseñó la Aritmética comercial básica, lo que despertó un gran interés por la Matemática. Conoció el sistema de numeración indo-arábigo y se dice que fue quien lo introdujo en Europa intentando sustituir la incómoda numeración romana, lo que debió bastar para reconocer su gran mérito.

En el año 1225 al pasar por la ciudad de Pisa el emperador Federico II quiso conocer al célebre sabio que en ella vivía y para que le mostrase sus habilidades se organizó un torneo matemático. Le plantearon tres problemas que Fibonacci resolvió con facilidad y publicó luego, junto a otros doce en su primer libro "Flor de soluciones de ciertas cuestiones relativas a los números y a la geometría". En ese libro aparecen por primera vez en Europa los números negativos entendidos como deudas.

El libro más conocido y por el que se le considera el primero de los matemáticos europeos medievales es el "Liber Abaci" publicado en 1202, donde, contrario a lo que su título sugiere, demuestra las ventajas de las cifras indo-arábigas frente a los que empleaban la antigua y complicada notación romana). Para comprender la lucha de Leonardo tómese en cuenta que cien años después de publicado el "Liber Abaci", los banqueros florentinos tenían prohibido utilizar las cifras indo-arábigas.

Varios capítulos del libro se dedican al planteamiento de problemas y acertijos, entre los que aparece el famoso problema de los conejos que todavía hoy a más de 800 años de distancia continúa asombrando con sus nuevas y curiosas propiedades.

La otra obra escrita por Leonardo fue el "Liber Quadratorum", sobre problemas y acertijos con números enteros cuadrados en la línea de la "Arithmetica" de Diofanto de Alejandría.

De su vida no se sabe mucho más. Murió en su ciudad natal en 1250. En el Camposanto del Duomo en Pisa se alza una imponente escultura de Leonardo Fibonacci, el primer gran maestro matemático europeo del medioevo. Es curioso que Fibonacci sea más conocido en la actualidad por el problema de los conejos que por ser quien introdujo en el mundo occidental las cifras indo-arábigas que hoy utilizamos.

8.5.2. Los números de Fibonacci

Anteriormente comentábamos que es irónico que Fibonacci se recuerde hoy en día gracias a que el teorista de números Edouard Lucas asignó su nombre en el siglo XIX

a una sucesión que aparece en un problema trivial del "Liber Abaci". Se trata del siguiente problema:

> "Un hombre colocó una pareja de conejos en un lugar totalmente rodeado por una pared ¿Cuántas parejas de conejos podrán producirse a partir de esa pareja en un año, si la naturaleza de esos conejos es tal que cada pareja produce en cada mes una nueva pareja de conejos, la cual se vuelve productiva a partir de su segundo mes de vida?"

Si se asume que no muere ningún conejo, entonces nace una nueva pareja en el primer mes. Durante el segundo mes, la pareja original produce una segunda pareja, pero la pareja que nació en el primer mes aún no es fértil. Un mes más tarde, tanto la pareja original como la primera que nació producen nuevas parejas, de manera que hay tres parejas adultas y dos jóvenes, y así sucesivamente. Las relaciones aparecen tabuladas a continuación. La idea a considerar es que cada mes la pareja joven crece y se vuelve adulta, de modo que los adultos son los que existían más los que dejan de ser jóvenes. Cada pareja que era adulta en el mes anterior produce una pareja joven, de modo que el número de parejas jóvenes coincide con el número previo de parejas adultas. Si se continúa indefinidamente, la sucesión que se obtiene en el problema de los conejos

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$$

se conoce como **sucesión de Fibonacci** y sus términos son los **números de Fibonacci**. La posición de cada número en la sucesión se denota por un subíndice, de modo que F_n es el n**-ésimo número de Fibonacci** y se tiene $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, etcétera.

Crecimiento de la colonia de conejos

Mes	Parejas adultas	Parejas jóvenes	Total
1	1	1	2
2	2	1	3
3	3	2	5
4	5	3	8
5	8	5	13
6	13	8	21
7	21	13	34
8	34	21	55
9	55	34	89
10	89	55	144
11	144	89	233
12	233	144	377

La sucesión de Fibonacci muestra una interesante propiedad; a saber

$$\begin{aligned} 2 &= 1+1 \quad \text{o} \quad F_3 = F_2 + F_1, \\ 3 &= 2+1 \quad \text{o} \quad F_4 = F_3 + F_2, \\ 5 &= 3+2 \quad \text{o} \quad F_5 = F_4 + F_3, \\ 8 &= 5+3 \quad \text{o} \quad F_6 = F_5 + F_4, \ldots \end{aligned}$$

Luego, se obtiene la regla general para $n \geq 3$ dada por

$$F_1 = F_2 = 1, \qquad F_n = F_{n-1} + F_{n-2}.$$

Es decir, cada término de la sucesión a partir del tercero es la suma de los dos precedentes. Tales sucesiones se conocen como **sucesiones recursivas**.

Se dice que la sucesión de Fibonacci es la primera sucesión recursiva conocida en el mundo matemático. El propio Fibonacci debe haber reconocido la naturaleza recursiva de esa sucesión, pero no fue hasta 1634, cuando la notación matemática había progresado lo suficiente, que Albert Girard escribió la fórmula.

Note que los términos consecutivos de la sucesión de Fibonacci que se han calculado son primos relativos. Eso no es accidental, como muestra el siguiente teorema:

Teorema 8.5.1

La sucesión de Fibonacci cumple que $(F_n, F_{n+1}) = 1$ *para todo* $n \geq 1$.

Demostración: Sea d un divisor común de F_n y F_{n+1}. Entonces d divide a su diferencia $F_{n-1} = F_{n+1} - F_n$. Del mismo modo se observa que $d|F_{n-2} = F_n - F_{n-1}$. Trabajando de manera sucesiva se obtiene que $d|F_{n-3}$, $d|F_{n-4}$, $\ldots$, $d|F_1 = 1$, por lo que tiene que ser $d = 1$. **Q.e.d.**

Como $F_3 = 2$, $F_4 = 5$, $F_5 = 13$ y $F_{11} = 89$ son números primos, se pudiera suponer que F_n es primo si el subíndice $n > 2$ lo es. Sin embargo, basta observar el caso de $F_{19} = 4181 = 37 \cdot 113$ para convencerse de lo contrario.

No solo no es posible predecir cuál F_n es primo, sino que tampoco se conoce si existen infinitos números primos de Fibonacci.

Ya se conoce que el máximo común divisor de dos enteros positivos se puede obtener tras aplicar al algoritmo de la división de Euclides en un número finito de pasos. Tal número de pasos puede ser muy grande para ciertos enteros. La proposición concreta plantea: Dado $n > 0$, existen enteros positivos a y b tales que se necesita realizar exactamente n divisiones en el algoritmo de la división de Euclides para

calcular (a, b). Para verificar tal afirmación basta considerar $a = F_{n+2}$ y $b = F_{n+1}$. El algoritmo de Euclides para calcular (F_{n+2}, F_{n+1}) conduce al sistema de ecuaciones

$$\begin{aligned} F_{n+2} &= 1 \cdot F_{n+1} + F_n \\ F_{n+1} &= 1 \cdot F_n + F_{n-1} \\ &\cdots \\ F_4 &= 1 \cdot F_3 + F_2 \\ F_3 &= 1 \cdot F_2. \end{aligned}$$

Es evidente que se necesitan n divisiones. De este desarrollo también se deduce que $(F_{n+2}, F_{n+1}) = 1$, lo cual confirma que los números de Fibonacci consecutivos son primos relativos.

Por ejemplo, para $n = 6$ es $F_8 = 21$, $F_7 = 13$ y $(21, 13) = 1$ se obtiene en 6 pasos, como muestra la siguiente secuencia de divisiones:

$$\begin{aligned} 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Una de las más asombrosas propiedades de la sucesión de Fibonacci es que el máximo común divisor de dos números de Fibonacci es a su vez un número de Fibonacci. Para comprobarlo se necesita la siguiente identidad

$$F_{m+n} = F_{m-1}F_n + F_m F_{n+1}. \tag{8.2}$$

Demostración: (Por inducción para m fijo) Para $n = 1$ se cumple la identidad, pues

$$F_{m+1} = F_{m-1}F_1 + F_m F_2 = F_{m-1} + F_m.$$

Supongamos que se cumple la identidad para todo $n \leq k$ e intentemos demostrarla para $n = k + 1$. Por la hipótesis de inducción es

$$\begin{aligned} F_{m+k} &= F_{m-1}F_k + F_m F_{k+1} \\ F_{m+k-1} &= F_{m-1}F_{k-1} + F_m F_k. \end{aligned}$$

Sumando ambas ecuaciones se tiene

$$F_{m+k} + F_{m+k-1} = F_{m-1}(F_k + F_{k-1}) + F_m(F_{k+1} + F_k).$$

Aplicando la definicón de los números de Fibonacci es

$$F_{m+k+1} = F_{m-1}F_{k+1} + F_mF_{k+2},$$

como se quería demostrar. **Q.e.d.**

Por ejemplo:

$$F_9 = F_{6+3} = F_5F_3 + F_6F_4 = 5 \cdot 2 + 8 \cdot 3 = 34.$$

El siguiente teorema resulta de gran interés.

TEOREMA 8.5.2 *F_{mn} es divisible por F_m para todos $m \geq 1$, $n \geq 1$.*

Demostración: (Por inducción en n) El resultado es obviamente válido para $n = 1$. Por hipótesis de inducción sea F_{mn} divisible por F_m para $n = 1, 2, \ldots, k$. Usando la fórmula (8.2) es

$$F_{m(k+1)} = F_{mk-1}F_m + F_{mk}F_{m+1}.$$

Como F_m divide a F_{mk}, el miembro derecho de la expresión enterior es divisible por F_m, de donde $F_m | F_{m(k+1)}$. **Q.e.d.**

En preparación para el cálculo de (F_m, F_n), se presenta el lema siguiente:

LEMA 8.5.1 *Si $m = qn + r$, entonces $(F_m, F_n) = (F_r, F_n)$.*

Demostración: Según la fórmula (8.2) es

$$(F_m, F_n) = (F_{qn+r}, F_n) = (F_{qn-1}F_r + F_{qn}F_{r+1}, F_n).$$

Por el teorema 8.5.2 y usando el hecho de que $(a + c, b) = (a, b)$ si $b|c$, se tiene

$$(F_{qn-1}F_r + F_{qn}F_{r+1}, F_n) = (F_{qn-1}F_r, F_n).$$

Para comprobar que $(F_{qn-1}F_r, F_n) = 1$, sea $d = (F_{qn-1}F_r, F_n)$. La relación $d|F_n$ y $F_n|F_{qn}$ implica que $d|F_{qn}$, con lo cual d es divisor común de los números sucesivos de Fibonacci F_{qn-1} y F_{qn}, los cuales son primos relativos, por lo que $d = 1$.

Resulta sencillo comprobar que si $(a, c) =$, entonces $(a, bc) = (a, b)$. Luego,

$$(F_m, F_n) = (F_{qn-1}F_r, F_n) = (F_r, F_n).$$

Q.e.d.

En estos momentos ya disponemos de las herramientas para demostrar el resultado esperado:

TEOREMA 8.5.3

El máximo común divisor de dos números de Fibonacci es un número de Fibonacci; específicamente es

$$(F_m, F_n) = F_d \quad con \quad d = (m, n).$$

Demostración: Sea $m \geq n$. Aplicando el algoritmo de Euclides se obtiene el sistema de ecuaciones

$$\begin{aligned} m &= q_1 n + r_1 \qquad 0 < r_1 < n \\ n &= q_2 n + r_2 \qquad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \qquad 0 < r_3 < r_2 \\ &\dots \\ r_{n-2} &= q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Por el lema anterior es

$$(F_m, F_n) = (F_{r_1}, F_n) = (F_{r_1}, (F_{r_2}) = \ldots = (F_{r_{n-1}}, F_{r_n}).$$

Como $r_n | r_{n-1}$, por el teorema 8.5.2 $F_{r_n} | F_{r_{n-1}}$ si $(F_{r_{n-1}}, F_{r_n}) = F_{r_n}$. Pero como r_n es el último resto no nulo en el algoritmo de la división de Euclides, es $r_n = (m, n)$, con lo cual queda demostrado el teorema. **Q.e.d.**

Resulta interesante que a partir de este resultado se obtiene el recíproco del teorema 8.5.2; en otras palabras, si F_n es divisible por F_m, entonces n es divisible por m. En efecto, si $F_m | F_n$, entonces es $(F_m, F_n) = F_m$. Pero según el teorema 8.5.3 $(F_m, F_n) = F_{(m,n)}$, por lo que $m | n$. Resumiendo se cumple:

COROLARIO 8.5.1

En la sucesión de Fibonacci $F_m | F_n$ si y solo si $m | n$ para $m \geq 2$.

Un ejemplo del teorema es el cálculo de $(F_{16}, F_{12}) = (987, 144)$. Por el algoritmo de Euclides es

$$\begin{aligned} 9871 &= 6 \cdot 144 + 123 \\ 144 &= 1 \cdot 123 + 21 \\ 123 &= 1 \cdot 21 + 18 \\ 21 &= 1 \cdot 18 + 3 \\ 18 &= 6 \cdot 3 + 0, \end{aligned}$$

de donde de $(987, 144) = 3$. Del teorema anterior es

$$(F_{16}, F_{12}) = F_4 = 3 = F_{(16,12)}.$$

Se presentan a continuación algunas identidades básicas referentes a los números de Fibonacci. Una de las proposiciones más sencillas se refiere a que la suma de los n primeros números de Fibonacci es igual a $F_{n+2} - 1$; es decir

$$\sum_{k=1}^{n} F_k = F_{n+2} - 1. \tag{8.3}$$

Por ejemplo, al sumar los 8 primeros números de Fibonacci se obtiene

$$1 + 1 + 2 + 3 + 5 + 8 + 13 + 21 = 54 = 55 - 1 = F_{10} - 1.$$

La situación general se obtiene al sumar las relaciones

$$\begin{aligned} F_1 &= F_3 - F_2 \\ F_2 &= F_4 - F_3 \\ F_3 &= F_5 - F_4 \\ &\cdots \\ F_{n-1} &= F_{n+1} - F_n \\ F_n &= F_{n+2} - F_{n+1}. \end{aligned}$$

Q.e.d.

Otra importante identidad es

$$F_n^2 = F_{n+1}F_{n-1} + (-1)^{n+1}, \qquad n \geq 2. \tag{8.4}$$

Por ejemplo, para $n = 6$ y $n = 7$ es

$$\begin{aligned} F_6^2 &= 8^2 = 13 \cdot 5 - 1 = F_7F_5 - 1, \\ F_7^2 &= 13^2 = 21 \cdot 8 - 1 = F_8F_6 + 1. \end{aligned}$$

Para demostrar la identidad 8.4 se parte de la identidad

$$\begin{aligned} F_n^2 - F_{n+1}F_{n-1} &= F_n(F_{n-1} + F_{n-2}) - F_{n+1}F_{n-1} \\ &= (F_n - F_{n+1})F_{n-1} + F_nF_{n-2} \\ &= (-1)(F_{n-1}^2 - F_nF_{n-2}). \end{aligned}$$

Repitiendo el argumento es

$$\begin{aligned} F_n^2 - F_{n+1}F_{n-1} &= (-1)(F_{n-1}^2 - F_nF_{n-2}) \\ &= (-1)^2(F_{n-2}^2 - F_{n-1}F_{n-3}). \end{aligned}$$

Luego de $n-2$ pasos se obtiene

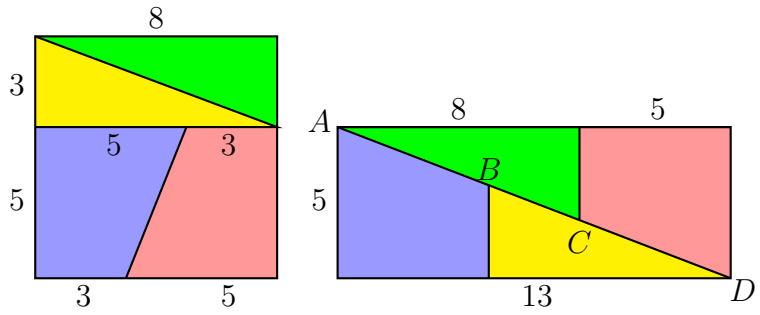
$$F_n^2 - F_{n+1}F_{n-1} = (-1)^{n-2}(F_2^2 - F_3F_1) = (-1)^{n-1}.$$

Q.e.d.

Para $n = 2k$ la identidad es

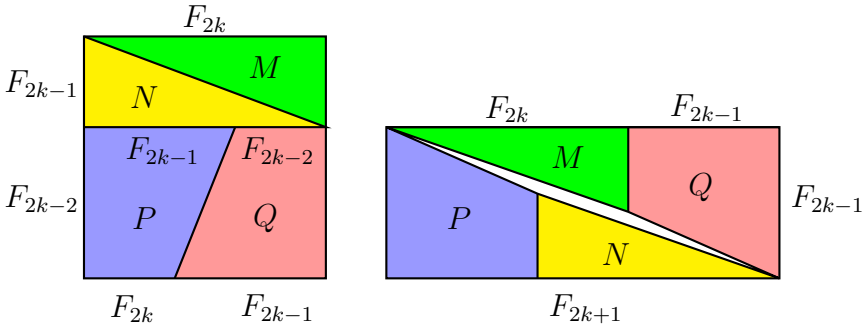
$$F_{2k}^2 = F_{2k+1}F_{2k-1} - 1.$$

Note que esta última identidad es la base para una conocido rompecabezas geométrico según el cual se descompone en piezas un cuadrado de 8 por 8 para obtener un rectángulo de 5 por 13.



El área del cuadrado es $8^2 = 64$ mientras que del rectángulo es $5 \cdot 13 = 65$, por lo que se incrementa el área en una unidad. La supuesta contradicción es sencilla de explicar, los puntos B, C no están sobre la diagonal $\overline{AB}$ del rectángulo .

Este tipo de rompecabezas se puede extender fácilmente a cualquier cuadrado cuyo lado sea un número de Fibonacci F_{2k}, como se muestra en la siguiente figura (se ha exagerado la imagen a la altura de la diagonal del rectángulo).



La identidad $F_{2k}^2 = F_{2k+1}F_{2k-1} - 1$ se puede interpretar como que el área del rectángulo menos el área del paralelogramo en el centro del rectángulo es precisamente el área del cuadrado original. Se puede comprobar que la altura del paralelogramo es

$$\frac{1}{\sqrt{F_{2k}^2 + F_{2k-2}^2}}.$$

Si F_{2k} es suficientemente grande (por ejemplo, $F_{2k} = 144$, de modo que $F_{2k-2} = 55$), la abertura que se forma en el centro del rectángulo es prácticamente imperceptible.

El siguiente resultado expresa que todo número entero positivo puede ser escrito como suma de números de Fibonacci, por ejemplo

$$\begin{array}{ll} 1 = F_1 & 5 = F_5 = F_4 + F_3 \\ 2 = F_3 & 6 = F_5 + F_1 = F_4 + F_3 + F_1 \\ 3 = F_4 & 7 = F_5 + F_2 + F_1 = F_4 + F_3 + F_2 + F_1 \\ 4 = F_4 + F_1 & 8 = F_6 = F_5 + F_4 \end{array}$$

Para demostrarlo basta comprobar por indución en $n > 2$ que cada uno de los enteros $1, 2, 3, \ldots, F_n - 1$ es suma de números del conjunto $\{F_1, F_2, \ldots, F_{n-2}\}$ sin repeticiones. Asumiendo que ello es válido para $n = k$ elegimos N tal que $F_k - 1 < N < F_{k-1}$. Como $N - F_{k-1} < F_{k+1} - F_{k-1} = F_k$. se infiere que el entero $N - F_{k-1}$ es suma de elementos diferentes de $\{F_1, F_2, \ldots, F_{n-2}\}$. Entonces N, y por tanto cada uno de los enteros $1, 2, 3, \ldots, F_n - 1$ puede ser expresado como suma (sin repeticiones) de elementos del conjunto $\{F_1, F_2, \ldots, F_{n-2}\}$. **Q.e.d.**

El siguiente teorema resume este resultado:

Teorema 8.5.4

Todo número entero positivo puede ser representado como suma finita sin repeticiones de números de Fibonacci.

8.5.3. Ejercicios

1. Dado un número primo $p \neq 5$ se conoce que F_{p-1} o F_{p+1} es divisible por p. Confírmelo para $p = 7, 11, 13, 17$.

2. Para $n = 1, 2, \ldots, 10$ demuestre que $5F_n^2 + 4(-1)^n$ es siempre un cuadrado perfecto.

3. Demuestre que si $2|F_n$, entonces $4|(F_{n+1}^2 - F_{n-1}^2)$, y si $3|F_n$, entonces se cumple que $9|(F_{n+1}^2 - F_{n-1}^2)$.

4. Para la sucesión de Fibonacci demuestre q ue:

   a) $F_{n+3} \equiv F_n \ (mod\ 2)$, por lo que F_3, F_6, F_9, ... son enteros pares.

   b) $F_{n+5} \equiv 3F_n \ (mod\ 5)$, por lo que F_5, F_{10}, F_{15}, ... son divisibles por 5.

5. Demuestre que la suma de los cuadrados de los primeros n números de Fibonacci está dada por la fórmula

$$F_1^2 + F_2^2 + \ldots + F_n^2 = F_n F_{n+1}.$$

   (Sugerencia: Para $n \geq 2$ es $F_n^2 = F_n F_{n+1} - F_n F_{n-1}$)

6. Utilice la identidad del problema 5 para probar que

$$F_{n+1}^2 = F_n^2 + 3F_{n-1}^2 + 2(F_{n-2}^2 + F_{n-1}^2 + \ldots + F_2^2 + F_1^2), \quad n \geq 3.$$

7. Calcule (F_9, F_{12}), (F_{15}, F_{20}) y (F_{24}, F_{36}).

8. Encuentre el número de Fibonacci que es divisor común de F_{24} y F_{36}.

9. Use el hecho de que $F_m | F_n$ si y solo si $m|n$ para comprobar las siguientes proposiciones:

   a) $2|F_n$ si y solo si $3|n$.

   b) $3|F_n$ si y solo si $4|n$.

   c) $4|F_n$ si y solo si $6|n$.

   d) $5|F_n$ si y solo si $5|n$.

10. Demuestre que si $(m, n) = 1$, entonces F_{mn} divide a $F_m F_n$ para todos $m, n \geq 1$.

11. Se puede demostrar que si F_n se divide por F_m $(m < n)$, entonces el resto r es un número de Fibonacci o $F_m - r$ es un número de Fibonacci. Encuentre ejemplos que ilustren ambos casos.

12. Se conjetura que existen solo 5 números de Fibonacci que son a su vez números triangulares. Hállelos.

13. Para $n \geq 1$ demuestre que $2^{n-1}F_n \equiv n \ (mod\ 5)$ (Sugerencia: Utilice la inducción y el hecho de que $2^n F_{n+1} = 2(2^{n-1}F_n + 4(2^{n-2}F_{n-1}))$

14. Usando inducción en n, demuestre la fórmula

$$F_1 + 2F_2 + 3F_3 + \ldots + nF_n = (n+1)F_{n+2} - F_{n+4} + 2.$$

15. *a)* Demuestre que para la suma de los primeros n números de Fibonacci con índice impar se cumple la fórmula

$$F_1 + F_3 + F_5 + \ldots + F_{2n-1} = F_{2n}.$$

(Sugerencia: Sume las igualdades $F_1 = F_2$, $F_3 = F_4 - F_2$, $F_5 = F_6 - F_4 \ldots$)

b) Demuestre que para la suma de los primeros n números de Fibonacci con índice par se cumple la fórmula

$$F_2 + F_4 + F_6 + \ldots + F_{2n} = F_{2n+1} - 1.$$

(Sugerencia: Utilice el inciso a) y la identidad 8.3)

c) Deduzca la siguiente expresión para la suma alternada de los primeros n números de Fibonacci

$$F_1 - F_2 + F_3 - F_4 + F_5 - F_6 + \ldots + (-1)^{n+1}F_n = 1 + (-1)^{n+1}F_{n-1}.$$

16. De la fórmula (8.3) deduzca para $n \geq 2$ que

$$F_{2n-1} = F_n^2 + F_{n-1}^2, \qquad F_{2n} = F_{n+1}^2 - F_{n-1}^2.$$

17. Demuestre para $n \geq 2$ la validez de la fórmula

$$F_n F_{n-1} = F_n^2 - F_{n-1}^2 + (-1)^n$$

Y concluya a partir de ello que los números de Fibonacci consecutivos son primos relativos.

18. Demuestre las siguientes identidades (evite usar inducción)

a) $F_{n+1}^2 - 4F_nF_{n-1} = F_{n-2}^2$ para $n \geq 3$ (Sugerencia: Comience por elevar al cuadrado las igualdades $F_{n-2} = F_n - F_{n-1}$ y $F_{n+1} = F_n + F_{n-1}$.)

b) $F_{n+1}F_{n-1} - F_{n+2}F_{n-2} = 2(-1)^n$ para $n \geq 3$ (Sugerencia: Utilice la formulación $F_{n+2} = F_n - F_{n+1}$ y $F_{n-2} = F_n - F_{n-1}$ y utilice la fórmula 8.4).)

c) $F_n^2 - F_{n+2}F_{n-2} = (-1)^n$ para $n \geq 3$ (Sugerencia: Imite la demostración de la fórmula 8.4).)

d) $F_nF_{n+1}F_{n+3}F_{n+4} = F_{n+2}^4 - 1$ para $n \geq 1$ (Sugerencia: Utilice c) y la fórmula 8.4).)

19. Represente los enteros 50, 75, 100 y 125 como suma de números de Fibonacci diferentes.

20. Demuestre que todo entero positive puede ser escrito como suma de dos términos diferentes de la sucesión $F_2, F_3, F_4, \ldots$.

21. Demuestre para $n \geq 1$ la identidad

$$(F_nF_{n+3})^2 + (2F_{n+1}F_{n+2})^2 = (F_{2n+3})^2.$$

Y úsela para generar 5 trios pitagóricos primitivos.

22. Demuestre que el producto $F_nF_{n+1}F_{n+2}F_{n+3}$ de cuatro números de Fibonacci consecutivos es el área de un triángulo pitagórico (Sugerencia: Utilice el resultado del problema anterior.)

23. Sea $\alpha = \frac{1}{2}(1+\sqrt{5})$ y $\beta = \frac{1}{2}(1-\sqrt{5})$, de modo que α y β son las raíces de la ecuación $x^2 = x+1$. Demuestre por inducción la **Fórmula de Binet** para $n \geq 1$

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

24. En 1876 Lucas encontró la siguiente fórmula para los números de Fibonacci en términos de los coeficientes binomiales

$$F_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \ldots + \binom{n-j}{j-1} + \binom{n-j-1}{j},$$

donde j es el mayor entero menor o igual que $\frac{n-1}{2}$. Demuéstrelo (Sugerencia: Argumente por inducción, utilice la relación

$$\binom{m}{k} = \binom{m-1}{k} + \binom{m-1}{k-1}$$

y la definición de F_n.)

25. Demuestre que

a) $$\binom{n}{1}F_1 + \binom{n}{2}F_2 + \binom{n}{3}F_3 + \ldots + \binom{n}{n}F_n = F_{2n}$$

b) $$-\binom{n}{1}F_1 + \binom{n}{2}F_2 - \binom{n}{3}F_3 + \ldots + (-1)^n\binom{n}{n}F_n = -F_n.$$

8.6. La ecuación de Pell

En enero de 1657 Fermat propuso a la comunidad matemática europea, pensando quizás en John Wallis, un par de problemas:

1. Halle un cubo que sumado a sus divisores propios sea un cuadrado.

2. Halle un cuadrado que sumado a sus divisores propios sea un cubo.

Uno de los favorites en la correspondencia de Fermat, Bernhard Frénicle de Bessy, encontró rápidamente varias respuestas al primer problema: por ejemplo: $(2\cdot3\cdot513\cdot4\cdot47)^3$ que incrementado en la suma de sus divisores propios produce $(2^7\cdot3^2\cdot5^2\cdot7\cdot13\cdot17\cdot29)^2$. Mientras tanto, Wallis consideraba que el problema no merecía sus esfuerzos. Pero el interés de Fermat estaba dirigido a la búsqueda de métodos y no de soluciones aisladas. Ambos Frénicle y Wallis subvaloraron el aspecto teórico del reto. En febrero de 1657 Fermat planteó su segundo reto, considerando directamente la parte teórica: hallar un número y que convierta a dy^2+1 en un cuadrado perfecto, siendo d un entero positivo que no es un cuadrado perfecto; por ejemplo, $3\cdot1^2+1=2^2$ y $5\cdot4^2+1=9^2$. Si no se puede encontrar la regla general, pedía Fermat, hallar el

menor valor de y que satisface la ecuación $61y^2 + 1 = x^2$ o $109y^2 + 1 = x^2$.

Pero ya se conoce que la Teoría de Números dejó de ser objeto de interés durante alrededor de un siglo hasta que Euler retomó los problemas planteados por Fermat. Euler y Lagrange contribuyeron a la resolución del problema de 1657. Al desarrollar $\sqrt{d}$ en una fracción continua infinita, Euler (1759) encontró un método para obtener la menor solución entera de $x^2 - dy^2 = 1$, pero no logró demostrar que el proceso condujera auna solución diferente de $x = 1$, $y = 0$. Quedó a Lagrange la resolución de este problema. Completando la teoría inconclusa de Euler, Lagrange publicó en 1768 la demostración rigurosa de que todas las soluciones se obtienen a partir del desarrollo de $\sqrt{d}$ en una fracción continua infinita. algunos autores suponen que Fermat poseía la solución completa del problema, puesto que más tarde el afirmó que utilizó con éxito su método del descenso infinito para mostrar la existencia de infinitas soluciones de $x^2 - dy^2 = 1$.

Como resultado de una referencia errónea (de Euler), la ecuación $x^2 - dy^2 = 1$ ha pasado a la historia con el nombre de "**ecuación de Pell**".

Para cualquier valor de d, la ecuación $x^2 - dy^2 = 1$ tiene la solución trivial $x = \pm 1$, $y = 0$. Si $d < -1$, entonces $x^2 - dy^2 \geq 1$ (excepto para $x = y = 0$), de modo que no hay más soluciones. Si $d = -1$, existen dos soluciones $x = 0$, $y = \pm 1$. El caso en que d es un cuadrado perfecto se elimina fácilmente: Si $d = n^2$, entonces $x^2 - dy^2 = 1$ puede escribirse en la forma

$$(x + ny)(x - ny) = 1,$$

lo cual es posible si y solo si $x + ny = x - ny = \pm 1$. Entonces es

$$x = \frac{(x - ny) + (x + ny)}{2} = \pm 1$$

y la ecuación no tiene más soluciones que las triviales $x = \pm 1$, $y = 0$.

Restringimos nuestra investigación de la ecuación de Pell $x^2 - dy^2 = 1$ al único caso de interés; es decir, al caso en que d es un entero positivo que no es cuadrado perfecto. Una solución x, y de la ecuación se llama **solución positiva** si ambos x e y son positivos. Es obvio que a partir de todas las soluciones positivas se obtienen las restantes soluciones mediante un reordenamiento de los signos $\pm x$, $\pm y$.

Los resultados siguientes mostrarán que todo par de enteros positivos que sean solución de la ecuación de Pell se obtienen a través del desarrollo de $\sqrt{d}$ en fracciones continuas.

Teorema 8.6.1

Si p, q son una solución positiva de $x^2 - dy^2 = 1$, entonces $\frac{p}{q}$ es una aproximación de la fracción continua de $\sqrt{d}$.

Demostración: Como $p^2 - dq^2 = 1$, se cumple

$$(p - q\sqrt{d})(p + q\sqrt{d}) = 1,$$

de donde $p > q\sqrt{d}$ y

$$\frac{p}{q} - \sqrt{d} = \frac{1}{q(p + q\sqrt{d})}.$$

Entonces

$$0 < \frac{p}{q} - \sqrt{d} < \frac{\sqrt{d}}{q(q\sqrt{d} + q\sqrt{d})} = \frac{\sqrt{d}}{2q^2\sqrt{d}} = \frac{1}{2q^2}.$$

De ello se deduce que $\frac{p}{q}$ tiene que ser una aproximación de la fracción continua de $\sqrt{d}$. **Q.e.d.**

En general el recíproco de este teorema no es válido; no todas las aproximaciones de la fracción continua de $\sqrt{d}$ son solución de la ecuación $x^2 - dy^2 = 1$. Sin embargo, algo se puede afirmar acerca de los valores de la sucesión $p_n^2 - dq_n^2$.

Teorema 8.6.2

Si $\frac{p}{q}$ es una aproximación de $\sqrt{d}$, entonces $x = p$, $y = q$ es una solución de una de las ecuaciones

$$x^2 - dy^2 = k,$$

donde $|k| < 1 + 2\sqrt{d}$.

Demostración: Si $\frac{p}{q}$ es una aproximación de $\sqrt{d}$, entonces se cumple que

$$\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2},$$

y por tanto

$$\left|p - q\sqrt{d}\right| < \frac{1}{q}.$$

Entonces

$$\left|p + q\sqrt{d}\right| = \left|(p - q\sqrt{d}) + 2q\sqrt{d}\right| < \frac{1}{q} + 2q\sqrt{d} < \left(1 + 2\sqrt{d}\right) q.$$

Combinando ambas desigualdades se obtiene

$$\left|p^2 - dq^2\right| = \left|p - q\sqrt{d}\right| \left|p + q\sqrt{d}\right| < \frac{1}{q}\left(1 + 2\sqrt{d}\right) q < \left(1 + 2\sqrt{d}\right),$$

que es lo que se quería demostrar. **Q.e.d.**

Como ejemplo veamos el caso $d = 7$. El desarrollo en fracciones continuas de $\sqrt{7}$ es $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$, las primeras aproximaciones son

$$\frac{2}{1}, \quad \frac{3}{1}, \quad \frac{5}{2}, \quad \frac{8}{3}, \ldots$$

Al calcular $p_n^2 - 7q_n^2$ se obtiene

$$2^2 - 7 \cdot 1^2 = -3, \quad 3^2 - 7 \cdot 1^2 = 2, \quad 5^2 - 7 \cdot 2^2 = -3, \quad 8^2 - 7 \cdot 3^2 = 1,$$

por lo que $x = 8$, $y = 3$ son una solución positiva de $x^2 - 7y^2 = 1$.

Respecto a la periodicidad de las fracciones continuas, el lector habrá notado en los ejemplos considerados que el desarrollo en fracciones continuas toma la forma

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_n}].$$

Es decir, el período comienza a partir del segundo término y el primer término es $\sqrt{d}$. También se cumple que $a_n = 2a_0$ y que el período, excluyendo el último término, es simétrico. Eso es típico de la situación general. Sin entrar en detalles de la demostración se cumple:

Si d es un entero positivo que no es cuadrado perfecto, entonces la fracción continua de $\sqrt{d}$ tiene la forma

$$\sqrt{d} = [a_0; \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}].$$

En el caso $d = 19$ se tiene

$$\sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}].$$

Mientras que para $d = 73$ es

$$\sqrt{73} = [8; \overline{1, 1, 5, 5, 1, 1, 16}].$$

Entre los números $d < 100$ el mayor período se obtiene para $\sqrt{94}$ que tiene 16 términos

$$\sqrt{94} = [9; \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}].$$

La siguiente tabla muestra los desarrollos en fracciones continuas de $\sqrt{d}$ para d entero no cuadrado entre 2 y 40.

$\sqrt{2} = [1; \overline{2}]$
$\sqrt{3} = [1; \overline{1, 2}]$
$\sqrt{5} = [2; \overline{4}]$
$\sqrt{6} = [2; \overline{2, 4}]$
$\sqrt{7} = [2; \overline{1, 1, 1, 4}]$
$\sqrt{8} = [2; \overline{1, 4}]$
$\sqrt{10} = [3; \overline{6}]$
$\sqrt{11} = [3; \overline{3, 6}]$
$\sqrt{12} = [3; \overline{2, 6}]$
$\sqrt{13} = [3; \overline{1, 4, 1, 6}]$
$\sqrt{14} = [3; \overline{1, 2, 1, 6}]$
$\sqrt{15} = [3; \overline{1, 6}]$
$\sqrt{17} = [4; \overline{8}]$
$\sqrt{18} = [4; \overline{4, 8}]$
$\sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}]$
$\sqrt{20} = [4; \overline{2, 8}]$
$\sqrt{21} = [4; \overline{1, 3, 1, 8}]$
$\sqrt{22} = [4; \overline{1, 2, 4, 2, 1, 8}]$
$\sqrt{23} = [4; \overline{1, 3, 1, 8}]$
$\sqrt{24} = [4; \overline{1, 8}]$
$\sqrt{26} = [5; \overline{10}]$
$\sqrt{27} = [5; \overline{5, 19}]$
$\sqrt{28} = [5; \overline{3, 2, 3, 10}]$
$\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$
$\sqrt{30} = [5; \overline{2, 10}]$
$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}]$
$\sqrt{32} = [5; \overline{1, 1, 1, 10}]$
$\sqrt{33} = [5; \overline{1, 2, 1, 10}]$
$\sqrt{34} = [5; \overline{1, 10}]$
$\sqrt{35} = [5; \overline{1, 10}]$
$\sqrt{37} = [6; \overline{12}]$
$\sqrt{38} = [6; \overline{6, 12}]$
$\sqrt{39} = [6; \overline{4, 12}]$
$\sqrt{40} = [6; \overline{3, 12}]$

El teorema 8.6.1 indica que si la ecuación $x^2 - dy^2 = 1$ tiene solución, entonces sus soluciones positivas se encuentran entre $x = p_k$, $y = q_k$, donde $\frac{p_k}{q_k}$ son las aproximaciones de $\sqrt{d}$. El período de la fracción continua de $\sqrt{d}$ contiene la información que se necesita para comprobar que $x^2 - dy^2 = 1$ realmente tiene solución en enteros, de hecho hay infinitas soluciones. La demostración se basa en el siguiente lema:

LEMA 8.6.1

Sean $\frac{p_k}{q_k}$ las aproximaciones de la fracción continua de $\sqrt{d}$. Si n es la longitud del período de la fracción continua de $\sqrt{d}$, entonces

$$p_{kn-1}^2 - d_{kn-1}^2 = (-1)^{kn} \quad (k = 1, 2, 3, \ldots).$$

Demostración: Para $k \geq 1$ se tiene

$$\sqrt{d} = [a_0; a_1, a_2, \ldots, a_{kn-1}, x_{kn}],$$

donde

$$x_{kn} = [2a_0; \overline{a_1, \ldots, a_{n-1}, 2a_0}] = a_0 + \sqrt{d}.$$

Del desarrollo anterior de $\sqrt{d}$ se deduce que

$$\sqrt{d} = \frac{x_{kn} p_{kn-1} + p_{kn-2}}{x_{kn} q_{kn-1} + q_{kn-2}}.$$

Sustituyendo $x_{kn} = a_0 + \sqrt{d}$ y simplificando, se reduce a

$$\sqrt{d}(a_0 q_{kn-1} + q_{kn-2} - p_{kn-1}) = a_0 p_{kn-1} + p_{kn-2} - d q_{kn-1}.$$

Como el miembro derecho es racional y $\sqrt{d}$ es irracional, la relación anterior requiere que sea

$$a_0 q_{kn-1} + q_{kn-2} = p_{kn-1} \quad \text{y} \quad a_0 p_{kn-1} + p_{kn-2} = d q_{kn-1}.$$

Al multiplicar la primera ecuación por p_{kn-1} y la segunda por por $-q_{kn-1}$ y sumarlas se obtiene

$$p_{kn-1}^2 - dq_{kn-1}^2 = p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2}.$$

Pero ya se conoce que

$$p_{kn-1}q_{kn-2} - q_{kn-1}p_{kn-2} = (-1)^{kn-2} = (-1)^{kn},$$

de modo que

$$p_{kn-1}^2 - dq_{kn-1}^2 = (-1)^{kn},$$

Lo que demuestra el lema. **Q.e.d.**

Ahora se pueden describir todas las soluciones positivas de $x^2 - dy^2 = 1$, donde $d > 0$ es un entero que no es cuadrado perfecto.

Teorema 8.6.3

Sean $\frac{p_k}{q_k}$ las aproximaciones de la fracción continua de $\sqrt{d}$. Y sea n la longitud del período de dicha fracción continua.

- *Si n es par, todas las soluciones positivas de la ecuación $x^2 - dy^2 = 1$ están dadas por*
$$x = p_{kn-1}, \quad y = q_{kn-1} \qquad (k = 1, 2, 3, \ldots).$$
- *Si n es impar, todas las soluciones positivas de la ecuación $x^2 - dy^2 = 1$ están dadas por*
$$x = p_{2kn-1}, \quad y = q_{2kn-1} \qquad (k = 1, 2, 3, \ldots).$$

Demostración: Ya se conoce que toda solución positiva de la ecuación $x^2 - dy^2 = 1$ es de la forma $x_0 = p_k$, $y_0 = q_k$ para cierta aproximación $\frac{p_k}{q_k}$.

Según el lema anterior $x = p_{kn-1}$, $y = q_{kn-1}$ conforman una solución si y solo si $(-1)^{kn} = 1$. Esa condición es válida para todo entero k si n es par. Si n es impar, la condición es válida cuando k es un entero par. **Q.e.d.**

EJEMPLO: Consideremos la ecuación $x^2 - 7y^2 = 1$. Como $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$ las primeras 12 aproximaciones son

$$\frac{2}{1}, \frac{3}{1}, \frac{5}{2}, \frac{8}{3}, \frac{37}{14}, \frac{45}{17},$$

$$\frac{82}{31}, \frac{127}{48}, \frac{590}{223}, \frac{717}{271}, \frac{1307}{494}, \frac{2024}{765}.$$

Como la longitud del período de la fracción continua es 4, el numerador y el denominador de toda aproximación $\frac{p_{4k-1}}{q_{4k-1}}$ constituye una solución de $x^2 - 7y^2 = 1$. Así

$$\frac{p_3}{q_3} = \frac{8}{3},\ \frac{p_7}{q_7} = \frac{127}{48},\ \frac{p_{11}}{q_{11}} = \frac{2024}{765}$$

se conforman las tres primeras soluciones positivas, que son

$$x_1 = 8, y_1 = 3;\ x_2 = 127, y_2 = 48;\ x_3 = 2024, y_3 = 765.$$

EJEMPLO: Para hallar las menores soluciones de $x^2 - 13y^2 = 1$ notemos que $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$ y el período es de longitud 5. Las primeras 10 aproximaciones son

$$\frac{3}{1}, \frac{4}{1}, \frac{7}{2}, \frac{11}{3}, \frac{18}{5},$$
$$\frac{119}{33}, \frac{137}{38}, \frac{256}{71}, \frac{393}{109}, \frac{649}{180}.$$

Entonces la menor solución positiva $x_1 = 649$, $y_1 = 180$ se obtiene a partir de la aproximación $\frac{p_9}{q_9} = \frac{649}{180}$.

Existe una forma rápida de generar otra solución a partir de una primera solución de la ecuación de Pell. Se llama **solución fundamental** de la ecuación $x^2 - dy^2 = 1$ a la menor solución positiva; es decir, la solución positiva x_0, y_0 con la propiedad de que $x_0 < x'$, $y_0 < y'$ para cualquier otra solución x', y'. Se conoce que, si la longitud del período de la fracción continua de $\sqrt{d}$ es n, entonces la solución fundamental de $x^2 - dy^2 = 1$ es $x = p_{n-1}$, $y = q_{n-1}$ si n es par, y $x = p_{2n-1}$, $y = q_{2n-1}$ si n es impar. Luego, la ecuación $x^2 - dy^2 = 1$ puede ser resuelta en n o $2n$ pasos.

Hallar la solución fundamental puede ser complicado, pues los números pueden ser muy grandes, aún para valores pequeños de d. Por ejemplo, la solución fundamental de la ecuación $x^2 - 991y^2 = 1$ es

$$\begin{aligned} x &= 379516400906811930638014896080 \\ y &= 12055735790331359447442538767. \end{aligned}$$

También puede suceder que la solución fundamental para un valor de d sea muy grande en comparación con la correspondiente al siguiente valor de d. Por ejemplo, la solución fundamental de la ecuación $x^2 - 61y^2 = 1$ es

$$x = 17663319094, \quad y = 22615398,$$

mientras que la solución fundamental de la ecuación $x^2 - 60y^2 = 1$ es $x = 31$, $y = 4$.

Con la ayuda de la solución fundamental (que puede ser calculada a través de las fracciones continuas o sustituyendo sucesivamente $y = 1, 2, \ldots$ en $1 + dy^2$ hasta obtener un cuadrado) estamos en condiciones de construir la restantes soluciones positivas.

Teorema 8.6.4

Sea x_1, y_1 la solución fundamental de la ecuación de Pell $x^2+dy^2=1$. Entonces todo para de enteros x_n, y_n con

$$x_n+y_n\sqrt{d}=\left(x_1+y_1\sqrt{d}\right)^n \qquad (n=1,2,3,\ldots)$$

es también una solución positiva de la ecuación de Pell.

Demostración: Resulta sencillo (queda como ejercicio al lector) comprobar que

$$x_n+y_n\sqrt{d}=\left(x_1+y_1\sqrt{d}\right)^2.$$

Como x_1, y_1 son positivos, también lo son x_n, y_n. Como x_1, y_1 son solución de la ecuación, se tiene

$$\begin{aligned} x_n^2-dy_n^2 &= \left(x_n+y_n\sqrt{d}\right)\left(x_n-y_n\sqrt{d}\right) \\ &= \left(x_1+y_1\sqrt{d}\right)^n\left(x_1-y_1\sqrt{d}\right)^n \\ &= \left(x_1^2-dy_1^2\right)^n=1^n=1, \end{aligned}$$

de modo que x_n, y_n. es una solución de la ecuación. **Q.e.d.**

EJEMPLO: Resulta fácil comprobar que $x_1=6$, $y_1=1$ es la solución fundamental de la ecuación $x^2-35y^2=1$. Una segunda solución positiva se obtiene de

$$x_2-y_2\sqrt{35}=\left(6+\sqrt{35}\right)^2=71+12\sqrt{35},$$

de donde que $x_2=71$, $y_2=12$. Esos enteros satisfacen la ecuación original, pues

$$71^2-35\cdot 12^2=5041-5040=1.$$

Una tercera solución positiva se obtiene de

$$x_3-y_3\sqrt{35}=\left(6+\sqrt{35}\right)^3=\left(71+12\sqrt{35}\right)\left(6+\sqrt{35}\right)=846+143\sqrt{35},$$

de donde que $x_3=846$, $y_3=143$ y de hecho es

$$846^2-35\cdot 143^2=715716-715715=1.$$

De vuelta a la ecuación $x^2+dy^2=1$, nuestro último teorema garantiza que la fórmula

$$x_n+y_n\sqrt{d}=\left(x_1+y_1\sqrt{d}\right)^2$$

permite calcular todas las soluciones positivas de la ecuación para n con valores enteros.

TEOREMA 8.6.5

Sea x_1, y_1 la solución fundamental de la ecuación de Pell $x^2+dy^2=1$. Entonces toda solución positiva de la ecuación está dada por enteros x_n, y_n con

$$x_n+y_n\sqrt{d}=\left(x_1+y_1\sqrt{d}\right)^n \qquad (n=1,2,3,\ldots).$$

Demostración: Supongamos que existe una solución positiva u, v que no se obtiene a partir de la fórmula $\left(x_1+y_1\sqrt{d}\right)^n$. Como $x_1+y_1\sqrt{d}>1$, sus potencias crecen indefinidamente, por lo que $u+v\sqrt{d}$ tiene que estar entre dos potencias consecutivas de $x_1+y_1\sqrt{d}$. Sea

$$\left(x_1+y_1\sqrt{d}\right)^n<u+v\sqrt{d}<\left(x_1+y_1\sqrt{d}\right)^{n+1},$$

O lo que es lo mismo

$$x_n+y_n\sqrt{d}<u+v\sqrt{d}<\left(x_n+y_n\sqrt{d}\right)\left(x_1+y_1\sqrt{d}\right).$$

De aquí se deduce que

$$1<\left(x_n-y_n\sqrt{d}\right)\left(u+v\sqrt{d}\right)<x_1+y_1\sqrt{d}.$$

Definimos ahora los enteros r y s mediante

$$r+s\sqrt{d}=\left(x_n-y_n\sqrt{d}\right)\left(u+v\sqrt{d}\right);$$

es decir,

$$r=x_nu-y_nvd, \qquad s=x_nv-y_nu.$$

Es fácil calcular que

$$r^2-ds^2=(x_n^2-dy_n^2)(u^2-dv^2)=1,$$

Por lo que r, s es una solución de $x^2-dy^2=1$ que cumple $0<r+s\sqrt{d}<1$. Entonces

$$\begin{aligned} 2r &= \left(r+s\sqrt{d}\right)+\left(r-s\sqrt{d}\right)>1+0>0 \\ sV &= \left(r+s\sqrt{d}\right)-\left(r-s\sqrt{d}\right)>1-1=0, \end{aligned}$$

por lo que r y s son positivos. Como x_1, y_1 es la solución fundamental de la ecuación de Pell $x^2+dy^2=1$, tiene que ser $x_1<r$, $y_1<s$, por lo que $x_1+y_1\sqrt{d}<r+s\sqrt{d}$, lo cual contradice una desigualdad anterior. **Q.e.d.**

8.6.1. Ejercicios

1. Si x_0, y_0 es una solución positiva de la ecuación $x^2 - dy^2 = 1$, demuestre que $x_0 > y_0$.

2. Por la técnica de sustituir sucesivamente $y = 1, 2, 3, \ldots$ en $dy^2 + 1$, halle la menor solución positiva de $x^2 - dy^2 = 1$ para d igual a

   (a) 7, (b) 11, (c) 18, (d) 30, (e) 39.

3. Halle todas la soluciones positivas de la siguiente ecuación con $y < 250$:

   (a) $x^2 - 2y^2 = 1$, (b) $x^2 - 3y^2 = 1$, (c) $x^2 - 5y^2 = 1$.

4. Muestre que existen infinitos enteros n con la propiedad de que ambos $n + 1$ y $\frac{n}{2} + 1$ son cuadrados perfectos. Presente dos ejemplos.

5. Calcule dos soluciones positivas de cada una de las siguientes ecuaciones

   (a) $x^2 - 23y^2 = 1$, (b) $x^2 - 26y^2 = 1$, (c) $x^2 - 33y^2 = 1$.

6. Calcule la solución fundamental de

   (a) $x^2 - 29y^2 = 1$, (b) $x^2 - 41y^2 = 1$, (c) $x^2 - 74y^2 = 1$. (Sugerencia: $\sqrt{41} = [6; \overline{2, 2, 12}]$, $\sqrt{74} = [8; \overline{1, 1, 1, 1, 16}]$.)

7. Halle una solución de cada una de las siguientes ecuaciones

   (a) $x^2 - 13y^2 = -1$, (b) $x^2 - 29y^2 = -1$, (c) $x^2 - 41y^2 = -1$.

8. Si x_0, y_0 es una solución de la ecuación $x^2 - dy^2 = -1$, demuestre que $x = 2x_0^2 + 1$, $y = 2x_0y_0$ satisface $x^2 - dy^2 = 1$. Brouncker utilizó este hecho para solucionar $x^2 - 313y^2 = 1$.

9. Si el número primo $p \equiv 3 \ (mod\ 4)$ divide a d, demuestre que la ecuación $x^2 - dy^2 = -1$ no tiene solución.

10. Si x_1, y_1 es la solución fundamental de la ecuación $x^2 - dy^2 = 1$ y

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n \qquad (n = 1, 2, 3, \ldots)$$

    demuestre que los enteros x_n, y_n se pueden calcular por la fórmula

$$\begin{aligned} x_n &= \frac{1}{2}\left[\left(x_1 + y_1\sqrt{d}\right)^n + \left(x_1 - y_1\sqrt{d}\right)^n\right] \\ y_n &= \frac{1}{2\sqrt{d}}\left[\left(x_1 + y_1\sqrt{d}\right)^n + \left(x_1 - y_1\sqrt{d}\right)^n\right]. \end{aligned}$$

11. Compruebe que los enteros x_n, y_n del problema anterior pueden ser definidos de manera inductiva para $n = 2, 3, \ldots$ mediante

$$\begin{aligned} x_{n+1} &= x_1 x_n + d y_1 y_n \\ y_{n+1} &= x_1 y_n + x_n y_1, \end{aligned}$$

o mediante

$$\begin{aligned} x_{n+1} &= 2x_1 x_n - x_{n-1} \\ y_{n+1} &= 2x_1 y_n - y_{n-1}. \end{aligned}$$

12. Sabiendo que la solución fundamental de $x^2 - 56y^2 = 1$ es $x_1 = 15$, $y_1 = 2$, halle dos soluciones más.

13. *a*) Demuestre que si la ecuación $x^2 - dy^2 = c$ tiene una solución, entonces tiene infinitas soluciones. (Sugerencia: Si u, v satisfacen la ecuación $x^2 - dy^2 = c$ y r, s satisfacen la ecuación $x^2 - dy^2 = 1$, entonces

$$(ur \pm dvs)^2 - d(us \pm vr)^2 = (u^2 - dv^2)(r^2 - ds^2) = c.\Big)$$

b) Si $x = 16$, $y = 6$ es una solución de $x^2 - 7y^2 = 4$, obtenga dos soluciones positivas más.

c) Si $x = 18$, $y = 3$ es una solución de $x^2 - 35y^2 = 9$, obtenga dos soluciones positivas más.

14. Aplique la teoría desarrollada en esta sección para comprobar que existen infinitos triplos pitagóricos x, y, z, en los cuales x e y son enteros consecutivos.

Bibliografía

[1] Apostol T. A.: *Introduction to Analytic Number Theory*. Springer Verlag. Berlin, Heidelberg, New York. 1976.

[2] Beker H. and Piper F.: *Cipher Systems*. Wiley. New York. 1982.

[3] Boyer C. B.; *A History of Mathematics*. Wiley. New York. 1968.

[4] Burton D. M.; *Elementary Number Theory*. Allyson and Bacon Inc. USA. 1980.

[5] Carmichael R. D.: *The Theory of Numbers and Diophantine Analysis*. Dover. New York. 1959.

[6] Dudley U.: *Elementary Number Theory*. Segunda edición. Freeman. New York. 1969

[7] Guy R. K.: *Unsolved Problems in Number Theory*. Springer Verlag. Berlin, Heidelberg, New York. 1981.

[8] Kurosch, A. G; *Álgebra Superior* Editorial Mir, Moscú, 1968.

[9] Loxton J. H. (editor): *Number Theory and Cryptography*. Cambridge University Pres. Cambridge. England. 1990.

[10] Noriega S$^{\acute{}}$anchez T, Piñeiro Díaz L.: *Álgebra*. Editorial Félix Varela. La Habana. 2007.

[11] Reguera Vilar R.,Solana Sagarduy M.: *Geometría Analítica*. Tercera Edición. Editorial Pueblo y Educación. La Habana. 2003.

[12] Sánchez, C. y Valdés, C.: *Las Funciones. Un paseo por su historia*. Editorial Nivola. Madrid. 2007.

[13] Sánchez, C. y Roldán, R.: *Goldbach. Una conjetura indomable*. Editorial Nivola. Madrid. 2009.

[14] Sánchez, C. y Roldán, R.: *Paseo por el universo de los números*. Editorial Academia. La habana. 2012.

[15] Sánchez, C. y Valdés, C.: *El entrañable encanto de las matemáticas*. Editorial Félix Varela. La Habana. 2010.

[16] Shanks D.: *Solved and Unsolved Problems in Number Theory*. Chelsea. New York. 1985.

[17] Sierpinski W.: 250 *Problems in Elementary Number Theory*. Polish Scientific Publishers. Warsaw. 1970.

[18] Sierpinski W.: *Elementary Theory of Numbers*. Pergamon Press. New York. 1964.

[19] Singh, S.: *El enigma de Fermat*. Editorial Planeta. Barcelona. 1998.

[20] Spiegel, M. R.; Moyer, R. E., *Álgebra Superior*. McGraw – Hill Interamericana, México, 2006.

[21] Turnbull, H. W.: *Grandes Matemáticos*. Editorial Científico-Técnica. La Habana. 1984.

[22] Valdés Castro C, Sánchez Fernńdez C.: *Introducción al Análisis Matemático*. Editorial Félix Varela. La Habana. 2011.

[23] Valdés Castro C, Sánchez Fernńdez C.: *Análisis de Funciones de una Variable Real*. Editorial Félix Varela. La Habana. 2017.

[24] Vinogradov M.: Fundamentos de la Teoría de los Números. Editorial MIR. Moscú. 1979.

[25] Wussing, H.: *Conferencias sobre Historia de la Matemática*. Editorial Pueblo y Educación. La Habana. 1989.

[26] Wussing, H. y Arnold, W.: *Biografías de grandes matemáticos*. Prensas Universitarias de Zaragoza. Universidad de Zaragoza. 1989.