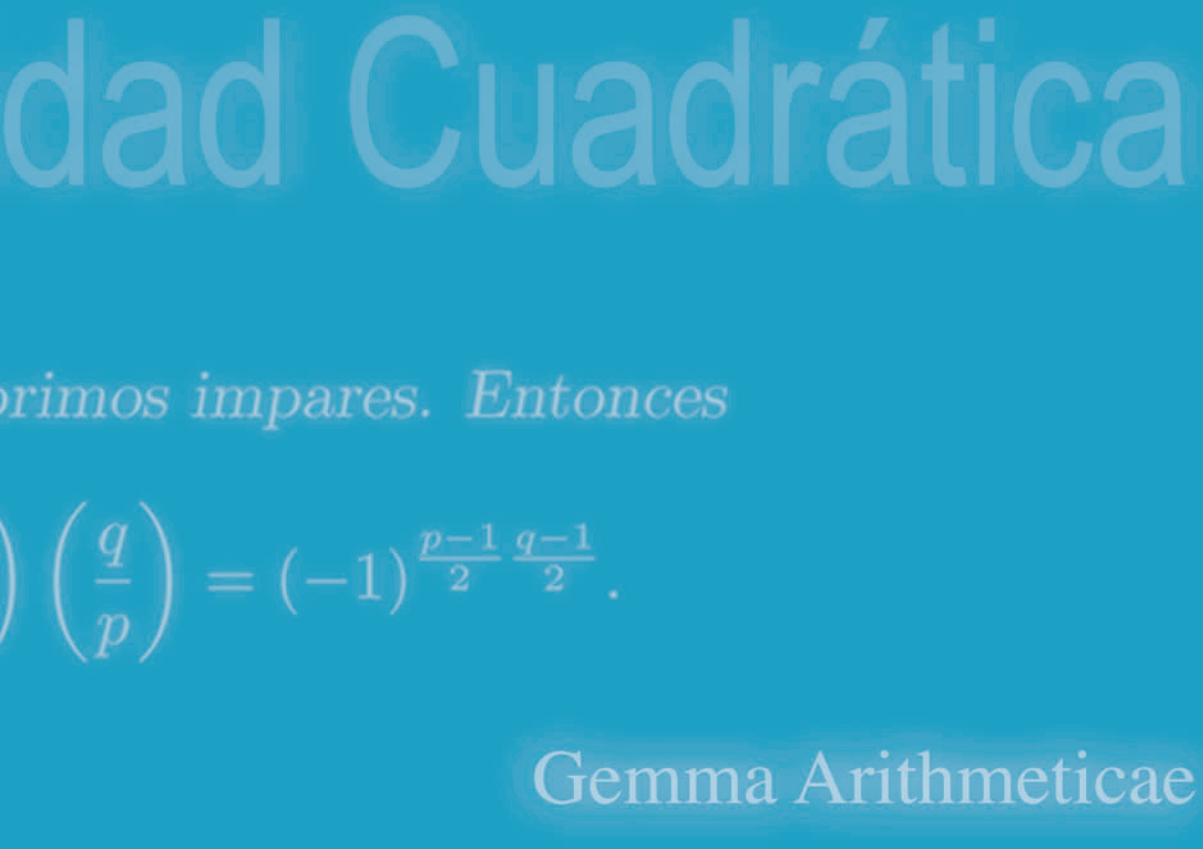
TEORÍA DE NÚMEROS

Antonio Cipriano Santiago Zaragoza



Gemma Arithmeticae

TEORÍA DE NÚMEROS

Antonio Cipriano Santiago Zaragoza

2009

TEORÍA DE NÚMEROS

Antonio Cipriano Santiago Zaragoza

2009

Vision Libros

Teoría de números
© Antonio Cipriano Santiago Zaragoza
© Editorial: Vision Libros
Calle San Benito 21 Local
Tel: 0034 91 3117696 url: www.visionlibros.com
Vision Libros es marca registrada de Vision Netware S.L.

ISBN: 978-84-9886-484-7
Descargado de: www.visionlibros.com

Diseño base cubierta: Marian González
reflejandoelazul@visionnet.es

Maquetación: Antonio Cipriano Santiago Zaragoza
daniel@visionnet.es

Distribuye y produce:
Distribuidora de publicaciones C/ Magnolias 35 Bis,
Local 28029 Madrid.

Pedidos a pedidos@visionnet.es
www.distribuciondepublicaciones.com

Reservados todos los derechos. Esta publicación no puede ser reproducida, ni registrada, sin el permiso previo por escrito de los titulares del copyright.

Índice general

Prólogo v

Prólogo del Autor ix

1. TEORÍA DE LA DIVISIBILIDAD **1**
1.1. Introducción 1
1.2. La relación de divisibilidad 2
1.3. Máximo común divisor 3
1.4. Mínimo común múltiplo 5
1.5. Algoritmo de la división 5
1.6. Identidad de Bezout 7
1.7. Teorema fundamental de la Aritmética 9
1.8. Algoritmo de Euclides 10

2. TEORÍA DE CONGRUENCIAS **15**
2.1. Definición y propiedades 15
2.2. El anillo $\mathbb{Z}_m$ 17
2.3. El teorema de Euler-Fermat 19
2.4. Congruencias lineales 22
2.5. Congruencias polinómicas módulo un primo 25
2.6. Algoritmo chino de los restos 26

3. LEY DE RECIPROCIDAD CUADRÁTICA **33**
3.1. Introducción 33
3.2. Concepto de resíduo cuadrático 34
3.3. El símbolo de Legendre 36
3.4. Infinitud de primos en progresiones aritméticas 44
3.5. Ley de reciprocidad cuadrática 47
3.6. El símbolo de Jacobi 55

4. EL GRUPO DE LAS UNIDADES DE $\mathbb{Z}_m$ **61**
4.1. Introducción 61
4.2. La estructura de $\mathcal{U}(\mathbb{Z}_m)$ para $m = p^e, 2p^e$ con p primo impar 63
4.3. La estructura del grupo $\mathcal{U}(\mathbb{Z}_{2^e})$ 66

4.4. El teorema de Carmichael 68

5. ELEMENTOS DISTINGUIDOS DE $\mathcal{U}(\mathbb{Z}_m)$ 73
5.1. Introducción 73
5.2. Resíduos cuadráticos 74
5.3. Idempotentes 75
5.4. Raíces cuadradas de la unidad 76

6. FACTORIZACIÓN 79
6.1. Introducción 79
6.2. Descomposición de un número conocida una raíz cuadrada de la unidad no trivial 79
6.3. Descomposición de un número conocido un idempotente no trivial 81
6.4. Ejemplo 82

7. TESTS DETERMINISTAS DE PRIMALIDAD 85
7.1. Introducción 85
7.2. El test de Wilson 87
7.3. Los tests de primalidad clásicos 89
7.4. Tests de primalidad para primos de Fermat 91
7.5. Algunos tests más eficientes de primalidad 94

8. TESTS DE PRIMALIDAD BASADOS EN SUCESIONES EN RECURRENCIA 97
8.1. Sucesiones de Lucas 97
8.2. Tests de Lucas y de Morrison 99
8.3. Números de Mersenne 101
8.4. Números perfectos 104

9. TESTS PROBABILÍSTICOS DE PRIMALIDAD 109
9.1. El test de Fermat 109
9.2. Números de Carmichael y pseudoprimos 110
9.3. Test de Solavay-Strassen 116
9.4. Test de Miller-Rabin 118
9.5. El teorema de Selfridge 121

10. EL ALGORITMO AKS 131
10.1. Introducción 131
10.2. El algoritmo AKS 132
10.3. Algoritmo AKS revisado 134
10.4. Algoritmo AKS "práctico" 134

Prólogo

Para cualquier lector atento toda aventura comienza por un prólogo. Es el primer escalón de un paseo por lo desconocido, el temblor inicial del festín prometido de la aventura. Porque un libro es siempre una aventura de índole muy diversa (intelectual, académica, laboral, sentimental, ociosa, divertida...).

El prólogo es una llave. Es un imán: te atrae y te desafía. Te adelanta algo del libro que tienes en las manos y te descubre un mundo de relaciones ajenas pero, al tiempo, complementarias entre el autor y su prologuista, entre el libro y su entorno. El prólogo ilumina, sitúa, complementa la obra en un universo de constelaciones que de otra forma no lograríamos alcanzar a menos que tuviéramos acceso a un conocimiento que la mayoría de las veces se nos escapa por ajeno y lejano.

¿Cuántas veces, leyendo un prólogo, nos hemos preguntado qué diríamos nosotros si el destino nos pusiera delante ese encargo comprometido? ¿Qué hubiéramos dicho de ese libro que tanto nos ha gustado y que hemos leído con deleite y asombro? ¿Y de su autor?

Aquí estoy yo con la ardua tarea de prologar el presente libro de matemáticas. Mi especialidad es otra, la lengua. ¿Qué relación hay entre la lengua y las matemáticas? Y, más aún, ¿cuál entre las matemáticas y la vida? Por definición, o más bien por consenso social las matemáticas se asocian tautológicamente a la exactitud: en el imaginario colectivo tiene demasiada fuerza la aritmética como disciplina originaria. Pero qué decir del caos, de la arbitrariedad y el azar, que también se nos presentan en lo diario como evidentes y que, sin embargo, oponen alguna resistencia a la formalización y el análisis. A pesar de las dificultades de aprehensión y definición matemáticas, esos conceptos son algo más que virtualidad, son un desafío. La vida juega revoltosamente y nos ofrece ejemplos magníficos.

Voy a ofrecer uno aunque, seguramente, este prólogo no vaya a suponer una clave en términos estrictamente académicos, pero sí en aspectos biográficos y sentimentales que relacionan al autor y al prologuista.

Mi pasión han sido siempre las matemáticas. Me tengo por un hombre apasionado, tal vez vehemente, al hablar, al expresar mis gustos o deseos, al defender mis posturas o argumentar mis convicciones. Mi entusiasmo era grande, si no desmesurado. Admiración primordial, emocional, casi mágica

por el dominio de los entresijos iniciales del edificio matemático (algo así como haber visto la entrada). Asombro proveniente no de lo conocido (un grano de arena) sino de lo intuido, de la inmensidad adivinada, del vasto horizonte al que era posible dirigirse.

Esta admiración de que hablo era palpable en mi casa: el hijo mayor iba a estudiar matemáticas, Ciencias Exactas que se decía entonces. Irradiándose como una fuerza invisible y desconocida la pasión matemática pasó a mi hermano Juanma (fui testigo de este hecho) pero no se detuvo ahí y pasó al hermano pequeño que dotado de una tremenda fuerza de voluntad, afrontó el reto, concluyó sus estudios y, desde entonces, se dedica a la enseñanza, además de atacar la tarea de escribir libros en sus ratos (escasos) libres. Siempre había sabido, quizás por la cercanía de edad, de esta atracción y entusiasmo en el primero. En cambio la decisión de Antonio Cipriano de dedicarse a la ciencia de los números fue toda una sorpresa y una ilusionada esperanza. Al fin y al cabo los hermanos mayores se ven un poco realizados (un poco a la manera de los padres) en los más pequeños.

Son las sorpresas que la vida y el azar nos tienen reservados: destinos distintos a los pronosticados, que no teníamos previstos.

Los escalones de las generaciones siguieron su terco ritmo, el prestigio de las matemáticas iniciado por el primer hermano, fue mantenido vivo por el tercero. Así llegó (debió llegar, o acaso deseo que así fuera) al hermano pequeño (el quinto) que no es otro que el autor de la obra que el lector tiene en sus manos. Y a mí no deja de parecerme curioso, fortuito, que una pasión y un deseo hayan saltado, ¿aleatoriamente?, de una voluntad a otra. Parece lo que no es: una casualidad.

No lo es. Si he empezado aludiendo al orden incierto que rige el azar, creyendo que era este el que había llevado a Antonio por el camino de la matemática, ahora observo con pasmo que los tres aludidos somos los hermanos 1, 3, 5. Un inicio de sucesión curioso del que podemos decir que sigue un orden regular pero se que se ha producido de manera inesperada (azarosa o aleatoria).

Lo dicho hasta aquí no tiene otro objeto que dejar constancia de la intensa admiración y el inmenso respeto que siento por mi hermano, autor de este volumen. Por ello es por lo que me enorgullece mostrarme como remotamente atañido por su trabajo y su éxito. Por ello aventuro un origen casi mítico e incierto para lo que vino después que no es otra cosa que el estudio constante y tenaz, la ilusión viva y la confianza reinventada día tras día, para llegar a ser un excelente profesor de matemáticas y un autor práctico, sencillo y coherente de manuales para estudiantes y amantes de esta disciplina o de profesionales que con ella se relacionan.

Así pues, no crea el lector que tiene en sus manos una obra del azar. Nada más lejos de la verdad. Este libro es fruto del trabajo decidido, de la reflexión oportuna y del tesón sin fatiga sobre todo del tesón. Del bien hacer, el esfuerzo continuo y silencioso, de la meticulosidad y la coherencia.

Aventúrese el lector, el profesional o el curioso y no quedarán defraudados.

Vayamos ahora a la introducción del contenido. Hagamos una síntesis sucinta.

En la teoría elemental de números, se estudian los números enteros sin emplear técnicas procedentes de otros campos de las matemáticas. A dicha teoría pertenecen, ente otras, las cuestiones de divisibilidad, el máximo común divisor, la factorización de los enteros como producto de números primos y, relacionado con todo lo anterior, la búsqueda de los números perfectos (número natural que es igual a la suma de sus divisores propios positivos sin incluirse él mismo) y las congruencias (que se dan cuando dos números enteros a y b tienen el mismo resto al dividirlos por un número natural m, llamado «módulo»).

De lo anterior constituyen enunciados típicos el pequeño teorema de Fermat y el teorema de Euler que lo extiende, el teorema chino del resto y la ley de reciprocidad cuadrática. En esta rama de la teoría de números se investigan también las propiedades de las funciones multiplicativas, como la función de Möbius y la función φ de Euler; así como las sucesiones de números enteros, tales como los factoriales y los números de Fibonacci.

Me propongo realizar un periplo por los elementos básicos que constituyen dicha teoría. Este itinerario vendrá determinado (con el límite superior de mi dominio de la materia) por mi experiencia personal marcada por percepciones y sentimientos subjetivos que no pueden dejar de relacionarse con el autor. Habrá igualmente algunas pinceladas sobre la evolución de la teoría de números a lo largo de la historia.

El presente texto, que hace una apuesta seria y sistemática sobre dicha teoría va dirigido a estudiantes, amantes de los números, de las matemáticas, y público en general, supone un paso más en la estructuración metodológica de dicho conocimiento y refleja a su autor como profesional trabajador metódico, riguroso y sólido.

En el estudio de las matemáticas uno no puede dejar de recordar los primero pasos, el acercamiento a los rudimentos de la adición y de la multiplicación (la famosa tabla de multiplicar) en definitiva un mundo que rápidamente se volvía complejo con relaciones en muchos casos pertenecientes al campo del álgebra, o de la propia teoría de números que marcaban un distingo en la percepción de la capacidad, o no, para el aprendizaje de dicho conocimiento: ¡A este niño se le dan bien las matemáticas! O su vertiente negativa, menos agradable. Eran las expresiones más comunes cuando tan sólo se había iniciado el camino para pasear por la playa, antes de siquiera tocar el agua del profundo océano del conocimiento matemático.

Eran partes de la matemática que quizás por acercarse a actividades de la vida cotidiana y por ser accesibles a un mayor porcentaje de la población podían ser entendidas y valoradas como un test de aptitud incuestionable.

Y ello es histórico. Fueron los matemáticos hindúes los que se interesaron por encontrar soluciones enteras a las ecuaciones diofánticas (se denomina así a cualquier ecuación algebraica, generalmente de varias variables, que se plantea sobre el conjunto de los números enteros $\mathbb{Z}$ o de los números naturales $\mathbb{N}$) desde la época de los Vedás.

Precisamente, el segundo de los conjuntos, el de los números naturales $\mathbb{N}$ constituye el primer acercamiento del niño a las matemáticas. Aprende a contar y comprende rápidamente la cadencia decenal que puede repetir hasta el infinito. Tal vez para su mente el infinito son mil, pero es el primer acercamiento al sentimiento de infinitud.

No es tan trivial, sin embargo, el conjunto de los números enteros $\mathbb{Z}$. La sustracción sería la tercera operación, la que nos acerca a ese ámbito. En el desafortunado caso de que el minuendo sea menor que el sustraendo el aprendiz se encuentra con un problema. Eso de que existan números negativos y que sean negativos pero con la misma dimensión que los positivos nos acerca a un mundo más abstracto. Por analogía, ha de existir un infinito también en esa dirección. ¿Será el mismo infinito que el anterior? ¿Será distinto? Nuevamente la historia nos dice que los matemáticos de la época jainia fueron los primeros en descartar la idea de que todos los infinitos son los mismos o iguales. Llegaron a reconocer hasta cinco tipos de infinitos distintos: infinito en una o dos direcciones (unidimensionales), infinito en superficies (bidimensional), infinito en todas partes (tridimensional) y perpetuamente infinito (en un número infinito de dimensiones). Pero salvo en lo relativo a los unidimensionales, los otros ya son palabras mayores. La adquisición del conocimiento no es ahora directa en función de las aptitudes del niño sino que necesita el apoyo sistemático del estudio.

Continuando con la teoría de números y la historia, dicha disciplina fue materia favorita entre los matemáticos griegos de Alejandría en Egipto a partir del siglo III a.C. y llegaron a tener conciencia del concepto de ecuación diofántica en algunos casos particulares.

Precisamente fue Diofanto el primer matemático helenístico que estudió estas ecuaciones. Investigó un método para encontrar las soluciones enteras de las ecuaciones lineales indeterminadas, ecuaciones en las que falta información suficiente para producir un conjunto único de respuestas discretas. La ecuación $x + y = 30$ puede servir de ejemplo.

Para la solución de este tipo de ecuaciones ha de haberse manejado con anterioridad y soltura la última de las operaciones, la división, que es la menos trivial y, sin embargo, la que se relaciona con el principio, con la primera de las materias, la divisibilidad, mencionada en primer lugar al inicio del prólogo.

Granada, marzo de 2009

José Santiago Zaragoza

Prólogo del Autor

Continuando con el prólogo de mi hermano José, así es como comienza este libro: estudiando la relación de divisibilidad, que es de vital importancia en el estudio de la Teoría de Números. En el primer capítulo se ven el algoritmo de la división, el llamado Teorema Fundamental de la Aritmética y el Algoritmo de Euclides para calcular el máximo común divisor de varios números, así como su expresión mediante una combinación lineal entera.

La Teoría de la Divisibilidad nos abre la puerta para explorar muchos problemas en Teoría de Números, pero como el objetivo final del presente trabajo es dar respuesta a la pregunta ¿es N un número primo?, se hace necesario estudiar la Teoría de Congruencias, que es un paso más en la Teoría de la Divisibilidad. Se estudian en este segundo capítulo las congruencias, y algunos de sus resultados más famosos e importantes, como son el Teorema de Euler-Fermat y el Algoritmo Chino de los Restos.

El estudio de la Ley de Reciprocidad Cuadrática es la continuación natural de las Congruencias, ya que para llegar a ella, hay que estudiar las congruencias cuadráticas. Se introducen aquí el símbolo de Legendre y de Jacobi, y se estudian sus propiedades. A partir de aquí el camino se diversifica, de forma que para llegar al objetivo, se pueden tomar varias rutas. Yo he elegido una, que es la de, en el capítulo cuatro, hacer una breve parada, para estudiar con cierto detalle el conjunto de las unidades del anillo de restos módulo m, para posteriormente, en el capítulo cinco, estudiar los resíduos cuadráticos, los idempotentes y las raíces cuadradas de la unidad en dicho grupo (lo que constituyen sus elementos distinguidos).

Esta breve parada, que no ha sido tal, nos permite estudiar, en el capítulo seis, la factorización de enteros en dos casos particulares, a saber: cuando se conoce una raíz cuadrada de la unidad no trivial y cuando se conoce un idempotente no trivial. Estos resultados serán usados de forma amplia en los capítulos que restan.

Los cuatro últimos capítulos del libro están dedicados al estudio de los tests de primalidad, comenzando por los tests deterministas (los que nos dicen si un número es primo o no), para posteriormente analizar los tests

basados en sucesiones recurrentes, que se aplican principalmente a números de forma especial, como lo son los de Mersenne.

El capítulo nueve describe algunos de los mejores tests de primalidad de los denominados probabilistas o de composición, ya que lo que permiten asegurar es si un número dado es compuesto. Se estudian en él el Algoritmo de Solovay-Strassen y, los de Miller y Rabin, que son los mejores tests de este tipo de que disponemos.

En un principio el libro terminaba aquí, pero después me decidí a añadir un décimo capítulo, en el que trato el Algoritmo AKS, que bien se podría haber introducido en el capítulo de los tests deterministas, pero que por su importancia teórica, aunque todavía no práctica, he decidido dejar para este capítulo final.

No quisiera terminar este prólogo sin agraderle *a mi mujer María José* su apoyo y su fe ciega en mis posibilidades para llevar a cabo este proyecto. Sin su ayuda, y sin su sacrificio, ya que me ha quitado mucho tiempo de estar con ella, este libro no habría llegado a buen puerto. También quisiera agradecer a mi hermano José el prólogo que me ha escrito, y que tanto me emociona.

Valdepeñas, abril de 2009

El Autor

A Cristina, "mi peque"