Introducción

Este libro pretende acercar de manera amena, aunque profunda, algunos temas importantes que se relacionan con el concepto fundamental de número, y transmitir algo de la invalorable experiencia que resulta hacer matemática.

Los cinco capítulos del libro se pueden leer en forma independiente y cada uno está presentado para que el lector pueda internarse en forma paulatina en los temas elegidos hasta alcanzar un elevado nivel de comprensión. La intención es dejarle a quien lea alguno de estos **relatos** una impresión distinta de la matemática y contribuir al desarrollo de su pensamiento lógico y crítico. Recorrer los capítulos superando los desafíos propuestos será una experiencia agradable que ayudará a apreciar la belleza y el poder de esta ciencia.

La matemática, considerada **el lenguaje del universo**, ocupa un lugar muy destacado en la cultura de la humanidad. El hombre desde sus orígenes hace matemática, ciencia ésta llena de vida y en constante crecimiento. En la matemática el valor de verdad es absoluto, el rigor de sus enunciados y la precisión de sus demostraciones son fundamentales y la imaginación y el desafío no encuentran límites. Estas distinguidas características pueden cautivar a quien se dé la oportunidad de apreciarlas.

Los capítulos tienen ejercicios y problemas que permitirán aprender y madurar los conceptos tratados, por lo que se recomienda hacerlos antes de ver las soluciones propuestas.

El **Capítulo 1** trata sobre las sorprendentes propiedades de los números primos, que son los ladrillos básicos sobre los cuales descansa la aritmética. Se presentan teoremas famosos sobre primos como el de Fermat, y problemas muy interesantes como el de la forma de factorear en primos un número cualquiera. Esto se hace en un marco histórico mostrando la manera en que ha ido evolucionando el saber humano sobre los números primos. En la última sección se incluye el uso de la computadora para factorear números compuestos, uno de los problemas más importantes en muchas áreas de la matemática, incluyendo la criptografía.

El **Capítulo 2** trata sobre conceptos y técnicas básicas de conteo, es decir formas de agrupar convenientemente conjuntos de objetos con el fin de poder calcular eficientemente la cantidad de elementos que tiene. El abordaje se realiza mediante la resolución de sucesivas situaciones problemáticas reales, seguidas de la formalización necesaria y unificadora de ideas.

Como primer problema se plantea el famoso **problema de matrimonios**, sobre las posibles maneras de sentar matrimonios alrededor de una mesa intercalando hombres y mujeres sin que se puedan sentar dos esposos juntos. Para poder resolverlo, hay que recurrir a los principios de adición y multiplicación, a las permutaciones, los arreglos, los conjuntos con repetición, y al **Principio de Inclusión-Exclusión**, que surgen como necesidad para resolver diversas situaciones más sencillas. En el Apéndice se incluye el **Principio del Palomar**, infaltable en un primer acercamiento al arte de contar.

El **Capítulo 3** trata sobre el infinito. El título puede parecer ambicioso, sin embargo, los objetivos son modestos: aprender **algo** sobre el infinito matemático. Éste es un tema que generalmente no es abordado en la escuela secundaria, donde se aprende que hay conjuntos infinitos pero no se plantea la posibilidad de comparar entre sí la cantidad de elementos que tienen distintos conjuntos infinitos. Es más común pensar que cuando algo es infinito no hay nada más que contar.

En los diálogos entre Clara y el Maestro se verá que, simplemente usando el concepto de **correspondencia biunívoca** entre dos conjuntos se puede elaborar una sólida teoría sobre las cantidades de elementos de conjuntos infinitos. Veremos que **hay infinitos tipos de infinito**s, y otras ideas que seguramente interesarán al lector tanto como a Clara, quien nos acompañará con sus preguntas y razonamientos a lo largo de esta aventura por el infinito.

El **Capítulo 4** está dedicado a la **aritmética modular**, una aritmética finita, es decir con un conjunto finito de números. En rigor hay una de estas aritméticas para cada natural mayor o igual que 2, y todas ellas tienen mucho que ver con la aritmética usual de los enteros. Esta aritmética es también llamada **aritmética cíclica** porque modeliza la aritmética de las horas del reloj, ejemplo que conocemos muy bien.

En este capítulo se encuentra la definición precisa de los elementos y operaciones de esta aritmética, hay ejemplos y también ejercicios que permiten adquirir un buen manejo de ella. Además, se muestran algunas aplicaciones interesantes como la deducción de las reglas de divisibilidad de enteros que se aprende en la escuela y la construcción de códigos sencillos para encriptar mensajes cuyo invento se le atribuye a Julio César.

Luego de esa breve introducción a la **criptografía**, es decir, a la ciencia de mandar mensajes secretos, en el **Capítulo 5** este tema se amplía. Se estudian las principales ideas de su desarrollo moderno y se ve cómo la matemática es de gran ayuda. Se verán algunos métodos históricos como el de **Vigenere** (donde se necesita algo de aritmética modular) y **Playfair o Hill** (en donde se usan matrices). También se estudiarán cifrados en bloque más modernos y se ilustrarán las características principales del estándar criptográfico actual y las razones matemáticas por las cuales es tan bueno. Se verán **cifrados de flujo** y una versión reducida del conocido **RC4**. Finalmente, se discutirá la criptografía de clave publica/privada, donde la aritmética modular será de gran importancia.

En el **Capítulo 6** están las resoluciones a todos los ejercicios y problemas planteados en los capítulos anteriores.