UNIVERSIDAD DE PUERTO RICO EN HUMACAO
DEPARTAMENTO DE MATEMÁTICAS

A.	Encabezado	Universidad de Puerto Rico en Humacao
B.	Nombre del curso	Teoría de Números para Maestros
C.	Codificación	MATE 4030
D.	Cantidad de horas/créditos	Tres (3) horas contacto[1] / Tres (3) créditos
E.	Requisitos o correquisitos y otros requerimientos	MATE 3018 o MATE 3172 o un curso equivalente

F. Descripción del curso

En matemáticas se conoce como Teoría de Números el estudio de los números naturales según la definición de Peano, sus propiedades y sus interrelaciones. Este curso cubre las nociones básicas de un curso clásico de teoría de números a nivel subgraduado y ofrece una visión de las aplicaciones modernas a la ciencia y la tecnología. Los temas a cubrirse son los siguientes: números naturales, sistemas de numeración, divisibilidad, números primos, congruencias o aritmética modular, ecuaciones diofantinas, fracciones continuas, criptografía, problemas clásicos.

G. Objetivos de aprendizaje

Objetivos Generales:

Al finalizar el curso los estudiantes podrán:

1) Reconocer los números naturales como los elementos fundamentales de la matemática.
2) Hacer pruebas usando inducción matemática y recursión.
3) Conocer los fundamentos de numeración posicional, los algoritmos fundamentales de
4) la aritmética y los problemas propios de la divisibilidad.
5) Conocer y aplicar los conceptos de primalidad y factorización.
6) Utilizar las herramientas de Teoría de Números en problemas de importancia contemporánea.

Objetivos Específicos:

Al finalizar el curso, los estudiantes podrán:

1) Enunciar los Axiomas de Peano.
2) Hacer pruebas usando inducción matemática y recursión.
3) Escribir números en diferentes sistemas de numeración.
4) Programar los algoritmos de cambio de base en una calculadora programable.
5) Reconocer divisores y múltiplos de un número.
6) Usar las propiedades del Máximo Común Divisor y del Mínimo Común Múltiplo para obtener propiedades de los números.
7) Encontrar tríos pitagóricos y determinar los tríos primitivos.

[1] Una hora contacto equivale a cincuenta (50) minutos.

8) Determinar si un número es primo o no usando algoritmos clásicos.
9) Saber probar la infinitud de los números primos.
10) Discutir sobre los primos de Mersenne y Fermat.
11) Programar algoritmos de primalidad en calculadora programable.
12) Factorizar números usando la calculadora.
13) Usar, justificar y producir criterios de divisibilidad elementales.
14) Aplicar la función de Euler, para determinar el número de divisores de un número.
15) Resolver congruencias lineales.
16) Resolver problemas aplicando el Teorema del Residuo Chino.
17) Plantear y resolver ecuaciones diofantinas.
18) Enumerar y explicar los teoremas de Lagrange y Wilson.
19) Explicar la ley de reciprocidad cuadrática.
20) Discurrir sobre el tema de criptografía y la necesidad de éste en la sociedad moderna.
21) Encriptar y decriptar mensajes usando sistemas criptográficos elementales.
22) Hacer criptografía de clave pública (RSA y Diffie-Hellman) con números relativamente grandes que puedan procesarse en una calculadora programable.

H. Bosquejo de contenido y distribución del tiempo

I. *Los números Naturales* *(4 horas)*
1) Definición
2) Postulados de Peano
3) Postulado de inducción matemática
4) Recursión
5) Propiedades de números naturales

II. *Sistemas de Numeración* *(5 horas)*
1) Historia de la numeración
2) Métodos clásicos
3) Sistema posicional
4) Cambio de base
5) Sistema binario y su aplicación en la computación moderna

III. *Divisibilidad* *(6 horas)*
1) Divisores y múltiplos
2) Máximos común divisor y Algorítmo de Euclides
3) El mínimo común múltiplo
4) Teorema fundamental de la aritmética
5) Factorización única
6) Tríos Pitagóricos
7) La función mayor entero

IV. *Números Primos y Compuestos* *(5 horas)*
1) La Criba de Eratóstenes
2) Pruebas de primalidad
3) Infinitud de los números primos
4) Criterios de divisibilidad
5) Algoritmos de factorización
6) Primos de Mersenne, Fermat y Primos gemelos

V. *Congruencias* *(5 horas)*
1) Propiedades elementales
2) Clases residuales y aritmética modular
3) Sistemas reducidos y la función de Euler
4) Congruencias lineales
5) Teorema del Residuo Chino
6) Ecuaciones diofantinas
7) Congruencias cuadráticas
8) Potencias de un entero módulo n
9) Pequeño Fermat y función de Euler

VI. *Criptografía* *(5 horas)*
1) Problema de integridad y autenticidad de información
2) El problema de encriptar y decriptar
3) Sistemas de Julio César, Matriciales, Exponenciales
4) Logaritmos discretos
5) Sistemas criptográficos de clave privada y clave pública
6) Sistemas modernos: RSA y Diffie-Hellman

VII. *Fracciones Continuas* *(5 horas)*
1) Introducción
2) Identidades básicas
3) Expansión de un número racional como fracción continua
4) Expansión de un número irracional como fracción continua

VIII. Problemas Clásicos y Modernos de Teoría de Números *(4 horas)*
1) El último teorema de Fermat
2) La conjetura de Ulam, de Goldbach y de primos gemelos

Nota: El total de horas en la distribución del tiempo es treinta y nueve (39). Las seis (6) horas restantes se dejan para las evaluaciones en el salón de clase.

Total 45 horas

I. Estrategias Instruccionales

Con miras a lograr los objetivos del curso, el profesor podrá realizar una combinación de algunas de las siguientes actividades: conferencia, demostraciones, discusión de problemas, promoción de la participación estudiantil, discusión de las asignaciones individuales o grupales, discusión de exámenes, resolución de problemas usando la calculadora, lecturas, grupos de discusión, y proyectos para explorar, verificar y hacer conjeturas utilizando la tecnología disponibles.

Además, el profesor podrá fomentar, promover o coordinar otras actividades que considere conveniente para lograr los objetivos del curso.

J. Recursos mínimos disponibles o requeridos

Los recursos mínimos para el ofrecimiento del curso:

1) Sala de clase para veinte (20) estudiantes
2) Computadora con proyector digital
3) Disponibilidad de por los menos dos (2) libros incluidos en la Bibliografía en la Biblioteca de la institución

K. Técnicas de evaluación

El estudiante debe ser evaluado en diferentes aspectos: conocimiento del tema, conceptos y hechos fundamentales de la teoría; capacidad para inferir, conjeturar y probar propiedades de números; y capacidad para manejar los conceptos y hechos básicos de la teoría.

En el curso podrán utilizarse los siguientes tipos de evaluaciones con su correspondiente peso porcentual en la calificación final:

Exámenes parciales (mínimo de dos)	25% cada uno (por ciento máximo)
Asignaciones (individuales y grupales)	25% conjunto (por ciento máximo)
Un examen final	25%

El peso porcentual de cada examen puede ser ajustado por el profesor siempre y cuando el peso del examen final sea de 25% en la nota final. El cómputo de la nota final incluirá como mínimo dos (2) exámenes parciales, el examen final y el conjunto de asignaciones individuales y grupales.

L. Acomodo razonable

Los estudiantes que requieran acomodo razonable deben visitar la Oficina de Servicios para la Población con Impedimentos (SERPI) y comunicarse con el profesor al inicio del semestre para planificar el acomodo necesario conforme a las recomendaciones de SERPI.

M. Integridad académica

El Artículo 6.2 del Reglamento General de Estudiantes de la UPR (Certificación Número. 13, 2009-2010 de la Junta de Síndicos) establece que "*la deshonestidad académica incluye, pero no se limita a: acciones fraudulentas, la obtención de notas o grados académicos valiéndose de falsas o fraudulentas simulaciones, copiar total o parcialmente la labor académica de otra persona, plagiar total o parcialmente el trabajo de otra persona, copiar total o parcialmente las respuestas de otra persona a las preguntas de un examen, haciendo o consiguiendo que otro tome en su nombre cualquier prueba o examen oral o escrito, así como la ayuda o facilitación para que otra persona incurra en la referida conducta*".

Cualquiera de estas acciones estará sujeta a sanciones disciplinarias en conformidad con el procedimiento disciplinario establecido en dicho reglamento.

N Sistema de calificación

La nota se adjudicará a base de la siguiente escala (porcentual):
100 - 90 A; 89 - 80 B; 79 - 65 C; 64 - 55 D; 54 – 0 F

O. Bibliografía

1) Anderson, J. A., & Bell, J. M., (1996), *Number Theory with Applications*, New Jersey: Prentice Hall.
2) Beutelspacher, A., (1994), *Cryptology*, Washington, D. C: The Mathematical Association of America.
3) Bressoud, D. M., (1989), *Factorization and Primality Testing*, New York: Springer-Verlag.
4) Burton, D. M., *Elementary Number Theory*, New York: MacGraw Hill Company.
5) Conway, J. H., & Guy, R. K., (1995), *The Book of Numbers*, New York: Spring-Verlag.
6) LeVeque, W. J., (1990), *Elementary Theory of* Number, Boston, MA: Addison-Wesley.
7) Long, C. T., (1987), *Elementary Introduction to Number Theory*, New Jersey: Prentice Hall, (Rev. Ed).
8) Silverman, J. H., (1997), *A Friendly Introduction to Number* Theory, New Jersey: Prentice Hall.

Responsables de las revisiones

- Alberto Cáceres (16 de diciembre de 1997)
- Marilú lebrón Vázquez (16 de marzo de 1999)
- Marilú Lebrón Vázquez (7 de mayo de 2007)
- Wilson Ruiz Torres (23 de septiembre de 2016)