



PLAN DE ESTUDIOS (PE): Licenciatura en Matemáticas Aplicadas

ÁREA: Álgebra

ASIGNATURA: Teoría de Números

CÓDIGO:

CRÉDITOS: 6

FECHA: Junio 2017



Nivel Educativo:	Licenciatura
Nombre del Plan de Estudios:	Licenciatura en Matemáticas Aplicadas
Modalidad Académica:	Presencial
Nombre de la Asignatura:	Teoría de Números
Ubicación:	Nivel Formativo
Correlación:	
Asignaturas Precedentes:	Introducción a las Estructuras Algebraicas
Asignaturas Consecuentes:	N/A

2. CARGA HORARIA DEL ESTUDIANTE

Concepto	Horas por semana		Total de horas por periodo	Total de créditos por periodo
	Teoría	Práctica		
Horas teoría y práctica (16 horas = 1 crédito)	5	0	100	6

3. REVISIONES Y ACTUALIZACIONES

Autores:	Academia de Matemáticas
Fecha de diseño:	1995
Fecha de la última actualización:	Marzo 2001
Fecha de aprobación por parte de la academia de área, departamento u otro.	Julio 2017
Revisores:	José Juan Angoa Amador, María de Jesús López Toriz, César Cejudo Castilla, Iván Fernando Vilchis Montalvo, Carlos Alberto López Andrade
Sinopsis de la revisión y/o actualización:	Se actualizó el contenido del curso con la incorporación de dos capítulos y se proporciona una descripción más detallada de cada capítulo. El primero de los capítulos que se incorporó es el Capítulo 4 cuyo contenido tiene importantes aplicaciones en las comunicaciones y la seguridad de la información y el segundo capítulo que se incorporó es el quinto en el cual se exhiben un par de



	aplicaciones en las que se utilizan diversos conceptos desarrollados en los capítulos previos, una de dichas aplicaciones ya estaba en el programa anterior. Finalmente cabe mencionar que también se actualizó la bibliografía.
--	--

4. PERFIL DESEABLE DEL PROFESOR (A) PARA IMPARTIR LA ASIGNATURA:

Disciplina profesional:	Matemático
Nivel académico:	Licenciatura
Experiencia docente:	0 años
Experiencia profesional:	0 años

5. PROPÓSITO: Esta materia tiene como objetivo establecer un puente entre temas clásicos y temas modernos que tienen aplicaciones actuales.

6. COMPETENCIAS PROFESIONALES:

1. Conocer una de las ramas de las Matemáticas más antiguas y que tiene múltiples aplicaciones en la actualidad.
2. Aprender a escribir formalmente argumentos matemáticos.
3. Relacionar esta teoría con las diferentes ramas de las matemáticas y las ciencias.
4. Comprender la literatura especializada en el fascinante mundo de los números.
5. Comprensión de una lengua extranjera (inglés, nivel técnico avanzado).



Unidad de Aprendizaje	Contenido Temático	Referencias
<p>1. Los números enteros, el máximo común divisor y los números primos</p>	<p>1.1. Divisibilidad 1.2. El algoritmo de la división 1.3. Representación de los enteros 1.4. El máximo común divisor 1.5. El algoritmo euclidiano 1.6. Números primos 1.7. La distribución de los números primos 1.8. El teorema fundamental de la aritmética</p>	<p>Kenneth H. Rosen, Elementary Number Theory and Its Applications, 6th Edition, Pearson Addison Wesley, (2010)</p> <p>Burton D. M., Elementary Number Theory, Seven Edition, McGraw-Hill, (2010)</p> <p>Davenport's H., The Higher Arithmetic An Introduction of the Theory of Numbers Eighth Edition, Cambridge University Press, (2008)</p> <p>Baldoni M. W, Ciliberto C. and Piacentini Cattaneo G. M., Elementary Number Theory,, Cryptography and Codes, Universitext, Springer-Verlag Berlin Heidelberg, (2009)</p> <p>Hardy G. H. and Wright E. M., An Introduction to the Theory of Numbers, Sixth Edition Revised by Heath-Brown D. R. and Silverman J. H., Oxford University Press, (2008)</p> <p>Niven I., Zuckerman H. S. and Montgomery H. L., An introduction to the Theory of Numbers, Fifth Edition, John Wiley and Sons, (1991)</p>
<p>2. Congruencias</p>	<p>2.1 La relación de congruencia módulo n y aritmética modular 2.2 Sistema completo de residuos módulo n 2.3 Exponenciación modular 2.4 Congruencias lineales 2.5 El pequeño Teorema de Fermat 2.6 El Teorema de Wilson 2.7 Sistema reducido de residuos módulo n</p>	<p>Kenneth H. Rosen, Elementary Number Theory and Its Applications, 6th Edition, Pearson Addison Wesley, (2010)</p> <p>Burton D. M., Elementary Number Theory, Seven Edition, McGraw-Hill, (2010)</p>



Unidad de Aprendizaje	Contenido Temático	Referencias
	2.8 El Teorema de Euler 2.9 Ecuaciones diofánticas lineales 2.10 El Teorema chino del residuo	<p>Davenport's H., The Higher Arithmetic An Introduction of the Theory of Numbers Eighth Edition, Cambridge University Press, (2008)</p> <p>Baldoni M. W, Ciliberto C. and Piacentini Cattaneo G. M,, Elementary Number Theory,, Cryptography and Codes, Universitext, Springer-Verlag Berlin Heidelberg, (2009)</p> <p>Hardy G. H. and Wright E. M., An Introduction to the Theory of Numbers, Sixth Edition Revised by Heath-Brown D. R. and Silverman J. H., Oxford University Press, (2008)</p> <p>Niven I., Zuckerman H. S. and Montgomery H. L., An introduction to the Theory of Numbers, Fifth Edition, John Wiley and Sons, (1991)</p>
3. Funciones multiplicativas	3.1 Definición y ejemplos de funciones aritméticas, funciones multiplicativas y completamente multiplicativas 3.2 Propiedades de las funciones multiplicativas 3.3 La Función ϕ de Euler y sus propiedades 3.4 La función sumatoria de una función aritmética 3.5 Fórmula de inversión de Möbius	<p>Kenneth H. Rosen, Elementary Number Theory and Its Applications, 6th Edition, Pearson Addison Wesley, (2010)</p> <p>Burton D. M., Elementary Number Theory, Seven Edition, McGraw-Hill, (2010)</p> <p>Baldoni M. W, Ciliberto C. and Piacentini Cattaneo G. M,, Elementary Number Theory,, Cryptography and Codes, Universitext, Springer-Verlag Berlin Heidelberg, (2009)</p> <p>Hardy G. H. and Wright E. M., An Introduction to the Theory of Numbers, Sixth Edition Revised by Heath-Brown D. R. and</p>

Benemérita Universidad Autónoma de Puebla
Vicerrectoría de Docencia
Dirección General de Educación Superior
Facultad de Ciencias Físico Matemáticas



Unidad de Aprendizaje	Contenido Temático	Referencias
		<p>Silverman J. H., Oxford University Press, (2008)</p> <p>Niven I., Zuckerman H. S. and Montgomery H. L., An introduction to the Theory of Numbers, Fifth Edition, John Wiley and Sons, (1991)</p>
<p>4. Raíces primitivas, índices y residuos cuadráticos</p>	<p>4.1 El orden de un entero módulo n y raíces primitivas</p> <p>4.2 Raíces primitivas para primos</p> <p>4.3 Números compuestos que tienen raíces primitivas</p> <p>4.4 El índice aritmético (logaritmo discreto) y sus propiedades. Potencias residuales.</p> <p>4.5 Residuos cuadráticos y residuos no cuadráticos</p> <p>4.6 La ley de la reciprocidad cuadrática.</p>	<p>Kenneth H. Rosen, Elementary Number Theory and Its Applications, 6th Edition, Pearson Addison Wesley, (2010)</p> <p>Burton D. M., Elementary Number Theory, Seven Edition, McGraw-Hill, (2010)</p> <p>Davenport's H., The Higher Arithmetic: An Introduction of the Theory of Numbers, Eighth Edition, Cambridge University Press, (2008)</p> <p>Baldoni M. W, Ciliberto C. and Piacentini Cattaneo G. M., Elementary Number Theory,, Cryptography and Codes, Universitext, Springer-Verlag Berlin Heidelberg, (2009)</p> <p>Hardy G. H. and Wright E. M., An Introduction to the Theory of Numbers, Sixth Edition Revised by Heath-Brown D. R. and Silverman J. H., Oxford University Press, (2008)</p> <p>Niven I., Zuckerman H. S. and Montgomery H. L., An introduction to the Theory of Numbers, Fifth Edition, John Wiley and Sons, (1991)</p>
<p>5. Aplicaciones (Los Enteros Gaussianos,</p>	<p>5.1 Enteros Gaussianos y primos Gaussianos</p> <p>5.2 El algoritmo de la división para los</p>	<p>Kenneth H. Rosen, Elementary Number Theory and Its Applications, 6th</p>



Unidad de Aprendizaje	Contenido Temático	Referencias
Criptosistemas de llave pública)	<p>enteros Gaussianos</p> <p>5.3 El máximo común divisor</p> <p>5.4 Teorema de factorización única</p> <p>5.5 Criptosistema, criptosistema de llave privada y criptosistema de llave pública</p> <p>5.6 El criptosistema RSA</p> <p>5.7 El criptosistema ElGamal La ley de la reciprocidad cuadrática.</p>	<p>Edition, Pearson Addison Wesley, (2010)</p> <p>Baldoni M. W, Ciliberto C. and Piacentini Cattaneo G. M., Elementary Number Theory,, Cryptography and Codes, Universitext, Springer-Verlag Berlin Heidelberg, 2009</p> <p>Koblitz N., A Course in Number Theory and Cryptography, Second Edition, Springer-Verlag, (1994)</p> <p>Burton D. M., Elementary Number Theory, Seven Edition, McGraw-Hill, (2010)</p> <p>van Tilborg, H. C. A., Fundamentals of Cryptology, 1st Edition, Kluwer Academic Publisher, (2003)</p>

8. ESTRATEGIAS, TÉCNICAS Y RECURSOS DIDÁCTICOS

Estrategias y técnicas didácticas	Recursos didácticos
<ul style="list-style-type: none"> • Exposición oral • Solución de Problemas • Exposición de proyectos • Uso de un Sistema Algebraico Computacional (CAS por sus siglas en inglés) para la solución de problemas 	<ul style="list-style-type: none"> • Pizarrón, plumones, proyector y laptop. • Impresos (textos): libros, fotocopias, periódicos, documentos. • Imágenes fijas proyectables (fotos)-diapositivas, fotografías. • Programas informáticos, por ejemplo del CAS wxmáxima, el cual es software libre.



Eje (s) transversales	Contribución de la asignatura
Formación Humana y Social	La matemática como actividad creativa nos conduce a un mejor conocimiento de la naturaleza del hombre.
Desarrollo de Habilidades en el uso de las Tecnologías de la Información y la Comunicación	Diversos programas computacionales están fundamentados por el profundo conocimiento del álgebra lineal, la cercanía a estas estructuras matemáticas nos introduce a problemas tecnológicos e informáticos.
Desarrollo de Habilidades del Pensamiento Complejo	La matemática como una forma abstracta de pensar al mundo, implica un desarrollo complejo del pensamiento.
Lengua Extranjera	Diversa bibliografía del tema está en inglés.
Innovación y Talento Universitario	La matemática siempre es innovación, en cualquiera de sus estados.
Educación para la Investigación	Cotidianamente la actividad matemática se realiza dentro de un formato de investigación.

10. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
▪ Exámenes	75%
▪ Exposiciones	25%
Total	100%

11. REQUISITOS DE ACREDITACIÓN

Estar inscrito como alumno en la Unidad Académica en la BUAP
Asistir como mínimo al 80% de las sesiones para tener derecho a exentar por evaluación continua y/o presentar el examen final en ordinario o extraordinario
Asistir como mínimo al 70% de las sesiones para tener derecho al examen extraordinario
Cumplir con las actividades académicas y cargas de estudio asignadas que señale el PE