



FORMATO DE CONTENIDO DE CURSO

FACULTAD DE: CIENCIAS DE LA EDUCACIÓN  
PROGRAMA DE: LICENCIATURA EN MATEMÁTICAS

PLANEACIÓN DEL CONTENIDO DE CURSO

1. IDENTIFICACIÓN DEL CURSO

NOMBRE	:	TEORÍA DE LOS NÚMEROS
CÓDIGO	:	22140
SEMESTRE	:	QUINTO
NUMERO DE CRÉDITOS	:	CUATRO
PRERREQUISITOS	:	TEORÍA DE CONJUNTOS
HORAS PRESENCIALES DE ACOMPañAMIENTO DIRECTO	:	4
ÁREA DE FORMACIÓN	:	PROFESIONAL
TIPO DE CURSO	:	PRESENCIAL
FECHA DE ACTUALIZACIÓN	:	AGOSTO 2016

2. DESCRIPCIÓN:

Se pretende que los estudiantes interioricen los conceptos básicos de la teoría de números: divisibilidad, primos, factorización y congruencias módulo de un entero  $n$ . de acuerdo al desarrollo de los temas, se presentarán algunas aplicaciones a las ciencias de la computación y criptografía, tales como el análisis del funcionamiento del criptosistema RSA.

3. JUSTIFICACIÓN



## FORMATO DE CONTENIDO DE CURSO

La teoría de números, la reina de las matemáticas, como Gauss la llamó, es tal vez la disciplina matemática más antigua y la que ha ejercido sobre los hombres de todas las épocas una fascinación más profunda. Está llena de problemas sin resolver, cuyos términos son perfectamente inteligibles para todos y que, sin embargo, han desafiado la sagacidad de los matemáticos más potentes durante siglos.

Además, la actual teoría de números se ha visto enriquecida con la aparición de las nuevas técnicas de computación automática, y los computadores pueden ser utilizados en ella experimentalmente, por ejemplo para comprobar que una conjetura es falsa, y también como una ayuda en los métodos de demostración allí donde los razonamientos se ramifican más allá de las posibilidades de la mente humana. Por tanto, en la formación del matemático actual, se exige la incursión de esta parte de las matemáticas.

### 4. PROPÓSITO GENERAL DEL CURSO

- Comprender los conceptos de divisibilidad y congruencias módulo un entero  $n$ :
- Aplicar los fundamentos y resultados básicos de la teoría de números en la búsqueda de solución de problemas o pruebas de la veracidad de proposiciones en el contexto de la teoría de números.
- Asignar significado a los principios fundamentales de la teoría de números un ámbito interdisciplinario.

### 5. COMPETENCIA GENERAL DEL CURSO

- Reconocer, asignar significados e interpretar los principios de la teoría de números, desde un contexto abierto y multidisciplinar.
- Combinar axiomas, definiciones, hipótesis, conceptos y relaciones pre-establecidas para realizar demostraciones, refutar o justificar enunciados en concordancia con los métodos de la teoría de números.
- Formular conjeturas plausibles en el marco de la teoría de números y relacionarlas con otras áreas del saber matemático.
- Resolver, mediante argumentaciones coherentes, problemas relacionados con teoría de números.
- Redactar informes de lecturas acerca del tema y justificar sus apreciaciones mediante la exposición verbal.



**FORMATO DE CONTENIDO DE CURSO**

## **6. PLANEACIÓN DE LAS UNIDADES DE FORMACIÓN**

- Clases magistrales.
- Talleres asistidos.
- Ejercicios en clase.
- Presentación y análisis del tema.
- Discusiones grupales sobre el tema.
- Exposiciones sobre temas asignados.
- Asignación de tareas.

## **7. BIBLIOGRAFÍA**

### **7.1. BÁSICA**

- Burton, David M. Elementary Number Theory. McGraw-Hill (6a Ed.) 2007.
- Judson L. Willian, Topics in Number Theory, Volumen 1, Addison-Wesley Publishing Company. 1965.

### **7.2. COMPLEMENTARIA**

- Luis R. Jiménez B. Jorge E. Gordillo A. Gustavo N. Rubiano O. Teoría de números para principiantes. Universidad Nacional de Colombia sede bogota 2004.

FORMATO DE CONTENIDO DE CURSO

IUNIDAD 1. DIVISIBILIDAD		TIEMPO: 3 semanas		
COMPETENCIA	CONTENIDOS	ESTRATEGIAS DIDACTICAS	INDICADORES DE LOGROS	ESTRATEGIAS EVALUATIVAS
<ul style="list-style-type: none"> <li>• Determinar con criterio el máximo común divisor.</li> <li>• Identificar el algoritmo de Euclides y el teorema fundamental de la aritmética.</li> <li>• Manejar el concepto de número primos.</li> <li>• Manejar con criterio los métodos de factorización y números de Fermat.</li> <li>• Identificar las ecuaciones diofantinas lineales.</li> </ul>	1.1 Máximo común divisor. 1.2 El algoritmo de Euclides. 1.3 Números primos. 1.4 El teorema fundamental de la aritmética. 1.5 Métodos de factorización y números de Fermat. 1.6 Ecuaciones diofantinas lineales.	<ul style="list-style-type: none"> <li>• Clases magistrales.</li> <li>• Talleres asistidos para la resolución de problemas.</li> <li>• Presentación y análisis del tema.</li> <li>• Discusiones grupales sobre el tema.</li> <li>• Exposiciones sobre temas asignados.</li> <li>• Ejercicios de fijación y aplicación.</li> <li>• Actividades extraclases en la</li> </ul>	<ul style="list-style-type: none"> <li>• Determina con criterio el máximo común divisor.</li> <li>• Identifica el algoritmo de Euclides y el teorema fundamental de la aritmética.</li> <li>• Maneja el concepto de número primos.</li> <li>• Maneja con criterio los métodos de factorización y números de Fermat.</li> <li>• Identifica las ecuaciones diofantinas</li> </ul>	Para la evaluación de la unidad se tendrá en cuenta: <ul style="list-style-type: none"> <li>• La participación en el desarrollo de la clase.</li> <li>• Informes de lecturas.</li> <li>• Sustentación de trabajos.</li> <li>• Pruebas escritas.</li> </ul>

Vo. Bo. Comité Curricular Si  No

FORMATO DE CONTENIDO DE CURSO

		plataforma SICVI	lineales.	
--	--	------------------	-----------	--

UNIDAD 2. CONGRUENCIAS		TIEMPO: 2 semanas		
COMPETENCIA	CONTENIDOS	ESTRATEGIAS DIDACTICAS	INDICADORES DE LOGROS	ESTRATEGIAS EVALUATIVAS
<ul style="list-style-type: none"> <li>Manejar con criterio el concepto de congruencias, su clasificación y aplicación.</li> </ul>	2.1 Congruencias módulo un entero $m$ . 2.2 Congruencias lineales. 2.3 Sistemas de congruencias lineales. El teorema chino del residuo. 2.4 Aplicaciones de congruencias: pruebas de divisibilidad, dígitos de verificación.	<ul style="list-style-type: none"> <li>Clases magistrales.</li> <li>Talleres asistidos para la resolución de problemas.</li> <li>Presentación y análisis del tema.</li> <li>Discusiones grupales sobre el tema.</li> <li>Exposiciones sobre temas asignados.</li> </ul>	Maneja con criterio el concepto de congruencias, su clasificación y su aplicación.	Para la evaluación de la unidad se tendrá en cuenta: <ul style="list-style-type: none"> <li>La participación en el desarrollo de la clase.</li> <li>Informes de lecturas.</li> <li>Sustentación de trabajos.</li> <li>Pruebas escritas.</li> </ul>

Vo. Bo. Comité Curricular Si  No

**FORMATO DE CONTENIDO DE CURSO**

		<ul style="list-style-type: none"> <li>Ejercicios de fijación y aplicación.</li> <li>Actividades extraclases en la plataforma SICVI</li> </ul>		
--	--	--	--	--

**UNIDAD 3. ALGUNAS CONGRUENCIAS ESPECIALES.**

**TIEMPO: 2 semanas**

COMPETENCIA	CONTENIDOS	ESTRATEGIAS DIDACTICAS	INDICADORES DE LOGROS	ESTRATEGIAS EVALUATIVAS
<ul style="list-style-type: none"> <li>Comprender y utilizar los teoremas de Fermat, Wilson y Euler.</li> <li>Manejar el concepto de Pseudo primos.</li> </ul>	3.1 El pequeño teorema de Fermat. 3.2 El teorema de Wilson. 3.3 El teorema de Euler. 3.4 Pseudo primos.	<ul style="list-style-type: none"> <li>Clases magistrales.</li> <li>Talleres asistidos para la resolución de problemas.</li> <li>Presentación y análisis del tema.</li> <li>Discusiones grupales sobre el</li> </ul>	<ul style="list-style-type: none"> <li>Comprende y utilizar los teoremas de Fermat, Wilson y Euler.</li> <li>Maneja el concepto de Pseudo primos.</li> </ul>	Para la evaluación de la unidad se tendrá en cuenta: <ul style="list-style-type: none"> <li>La participación en el desarrollo de la clase.</li> <li>Informes de lecturas.</li> </ul>

Vo. Bo. Comité Curricular Si  No

**FORMATO DE CONTENIDO DE CURSO**

		<p>tema.</p> <ul style="list-style-type: none"> <li>• Exposiciones sobre temas asignados.</li> <li>• Ejercicios de fijación y aplicación.</li> <li>• Actividades extraclases en la plataforma SICVI</li> </ul>		<ul style="list-style-type: none"> <li>• Sustentación de trabajos.</li> <li>• Pruebas escritas.</li> </ul>
--	--	--	--	--

UNIDAD 4. FUNCIONES ARITMÉTICAS			TIEMPO: 2 semanas	
COMPETENCIA	CONTENIDOS	ESTRATEGIAS DIDACTICAS	INDICADORES DE LOGROS	ESTRATEGIAS EVALUATIVAS
<ul style="list-style-type: none"> <li>• Manejar el concepto de la función Euler.</li> <li>• Identificar los números perfectos y primos de Mersenne.</li> </ul>	<p>4.1 La función <math>\phi</math> de Euler.</p> <p>4.2 La suma de los divisores de un número. Números perfectos, primos</p>	<ul style="list-style-type: none"> <li>• Clases magistrales.</li> <li>• Talleres asistidos para la resolución de problemas.</li> <li>• Presentación y</li> </ul>	<ul style="list-style-type: none"> <li>• Maneja el concepto de la función Euler.</li> <li>• Identifica los números perfectos y primos de</li> </ul>	<p>Para la evaluación de la unidad se tendrá en cuenta:</p> <ul style="list-style-type: none"> <li>• La participación en el desarrollo de la clase.</li> </ul>

Vo. Bo. Comité Curricular Si  No

**FORMATO DE CONTENIDO DE CURSO**

<ul style="list-style-type: none"> <li>Comprender y utilizar la fórmula de inversión de Mobius.</li> </ul>	<p>de Mersenne, el Teorema de Euclides-Euler.</p> <p>4.3 Fórmula de inversión de Mobius</p>	<p>análisis del tema.</p> <ul style="list-style-type: none"> <li>Discusiones grupales sobre el tema.</li> <li>Exposiciones sobre temas asignados.</li> <li>Ejercicios de fijación y aplicación.</li> <li>Actividades extraclases en la plataforma SICVI</li> </ul>	<p>Mersenne.</p> <ul style="list-style-type: none"> <li>Comprende y utiliza la fórmula de inversión de Mobius.</li> </ul>	<ul style="list-style-type: none"> <li>Informes de lecturas.</li> <li>Sustentación de trabajos.</li> <li>Pruebas escritas.</li> </ul>
--	---	--	---	---

**UNIDAD 5. CRIPTOGRAFÍA**

**TIEMPO: 3 semanas**

COMPETENCIA	CONTENIDOS	ESTRATEGIAS DIDACTICAS	INDICADORES DE LOGROS	ESTRATEGIAS EVALUATIVAS
<ul style="list-style-type: none"> <li>Reconocer algunos métodos de encriptamiento de</li> </ul>	<p>5.1 Algunos métodos de encriptamiento de mensajes.</p>	<ul style="list-style-type: none"> <li>Clases magistrales.</li> <li>Talleres asistidos</li> </ul>	<ul style="list-style-type: none"> <li>Reconoce algunos métodos de encriptamiento de</li> </ul>	<p>Para la evaluación de la unidad se tendrá en</p>

Vo. Bo. Comité Curricular Si  No

**FORMATO DE CONTENIDO DE CURSO**

<p>mensajes.</p> <ul style="list-style-type: none"> <li>• Manejar las aplicaciones de la criptografía.</li> </ul>	<p>5.2 Criptografía de clave pública. 5.3 Protocolos criptográficos y aplicaciones.</p>	<p>para la resolución de problemas.</p> <ul style="list-style-type: none"> <li>• Presentación y análisis del tema.</li> <li>• Discusiones grupales sobre el tema.</li> <li>• Exposiciones sobre temas asignados.</li> <li>• Ejercicios de fijación y aplicación.</li> <li>• Actividades extraclases en la plataforma SICVI</li> </ul>	<p>mensajes.</p> <ul style="list-style-type: none"> <li>• Maneja las aplicaciones de la criptografía.</li> </ul>	<p>cuenta:</p> <ul style="list-style-type: none"> <li>• La participación en el desarrollo de la clase.</li> <li>• Informes de lecturas.</li> <li>• Sustentación de trabajos.</li> <li>• Pruebas escritas.</li> </ul>
---	---	---	--	--

FORMATO DE CONTENIDO DE CURSO

UNIDAD 6. RAÍCES PRIMITIVAS		TIEMPO: 2 semanas		
COMPETENCIA	CONTENIDOS	ESTRATEGIAS DIDACTICAS	INDICADORES DE LOGROS	ESTRATEGIAS EVALUATIVAS
<ul style="list-style-type: none"> <li>Determinar cuándo un número tiene raíces primitivas y las halla.</li> <li>Probar la primalidad de un número.</li> </ul>	<p>6.1 El orden de un entero módulo <math>m</math> y raíces primitivas.</p> <p>6.2 Raíces primitivas para primos.</p> <p>6.3 La existencia de raíces primitivas.</p> <p>6.4 Pruebas de primalidad, usando el orden de un entero y raíces primitivas.</p>	<ul style="list-style-type: none"> <li>Clases magistrales.</li> <li>Talleres asistidos para la resolución de problemas.</li> <li>Presentación y análisis del tema.</li> <li>Discusiones grupales sobre el tema.</li> <li>Exposiciones sobre temas asignados.</li> <li>Ejercicios de fijación y aplicación.</li> </ul>	<ul style="list-style-type: none"> <li>Determina cuándo un número tiene raíces primitivas y las halla.</li> <li>Prueba la primalidad de un número.</li> </ul>	<p>Para la evaluación de la unidad se tendrá en cuenta:</p> <ul style="list-style-type: none"> <li>La participación en el desarrollo de la clase.</li> <li>Informes de lecturas.</li> <li>Sustentación de trabajos.</li> <li>Pruebas escritas.</li> </ul>

FORMATO DE CONTENIDO DE CURSO

- Actividades extraclases en la plataforma SICVI

UNIDAD 7. RECIPROCIDAD CUADRÁTICA

TIEMPO: 2 semanas

COMPETENCIA	CONTENIDOS	ESTRATEGIAS DIDACTICAS	INDICADORES DE LOGROS	ESTRATEGIAS EVALUATIVAS
<ul style="list-style-type: none"> <li>• Identificar las congruencias polinomiales y cuadráticas.</li> <li>• Reconocer los símbolos de Legendre y Jacobi.</li> <li>• Entender la ley de reciprocidad cuadrática.</li> </ul>	7.1 Congruencias polinomiales. 7.2 Congruencias cuadráticas. Residuos cuadráticos. 7.3 El símbolo de Legendre. 7.4 El símbolo de Jacobi. 7.5 La ley de reciprocidad cuadrática.	<ul style="list-style-type: none"> <li>• Clases magistrales.</li> <li>• Talleres asistidos para la resolución de problemas.</li> <li>• Presentación y análisis del tema.</li> <li>• Discusiones grupales sobre el tema.</li> <li>• Exposiciones sobre temas asignados.</li> <li>• Ejercicios de fijación</li> </ul>	<ul style="list-style-type: none"> <li>• Identifica las congruencias polinomiales y cuadráticas.</li> <li>• Reconoce los símbolos de Legendre y Jacobi.</li> <li>• Entiende la ley de reciprocidad cuadrática.</li> </ul>	Para la evaluación de la unidad se tendrá en cuenta: <ul style="list-style-type: none"> <li>• La participación en el desarrollo de la clase.</li> <li>• Informes de lecturas.</li> <li>• Sustentación de trabajos.</li> <li>• Pruebas escritas.</li> </ul>

Vo. Bo. Comité Curricular Si  No



Universidad  
del Atlántico

CÓDIGO: FOR-DO-020

VERSIÓN: 0

FECHA: 03/08/2016

**FORMATO DE CONTENIDO DE CURSO**

		y aplicación. <ul style="list-style-type: none"><li>• Actividades extraclases en la plataforma SICVI</li></ul>		
--	--	---	--	--

Vo. Bo. Comité Curricular Si  No