DEPARTAMENTO DE MATEMATICAS
MATE-1103-Teoría de números.
Primer Semestre de 2021

César Galindo
Cn.galindo1116@uniandes.edu.co

- **Información de los profesores**

https://matematicas.uniandes.edu.co/index.php/cartelera/cursos-sem-actual

- **INTRODUCCIÓN Y DESCRIPCIÓN GENERAL DEL CURSO:**

Este curso es una introducción a algunos de los principales resultados, preguntas e ideas de la teoría de números clásica. Comenzaremos adquiriendo conocimiento de las herramientas y conceptos básicos en Teoría de Números tales como enteros, primos, divisibilidad, GCD, congruencias, teorema de Wilson y Fermat, pseudoprimos y funciones multiplicativas (como la función phi de Euler). Después, pasaremos a temas más avanzados, como criptografía y Seguridad informática, residuos cuadráticos, fracciones continuas. Estudiaremos aspectos computacionales y algorítmicos de cada tema según corresponda.

- **OBJETIVOS DE LA ASIGNATURA**

  - Entender como construir ideas matemáticas profundas usando bases simples.
  - Escribir y entender argumentos matemáticos.
  - Ampliar la visión de la riqueza de las matemáticas

- **COMPETENCIAS A DESARROLLAR**

Al completar con éxito este curso, los estudiantes están en capacidad de:

1. Conocimiento y comprensión de temas que incluyen, pero no se limitan a, divisibilidad, números primos, congruencias, reciprocidad cuadrática, criptografía.
2. Entender los métodos y técnicas utilizados en teoría de números elemental.
3. Escribir programas/funciones para calcular funciones propias de la teoría de números.
4. Escribir una demostración en forma correcta.

- **Metodología**

César Galindo
Cn.galindo1116@uniandes.edu.co

- Para aprender matemáticas es necesario un trabajo activo personal. Esto implica preparar cada clase con la ayuda del texto y hacer los ejercicios sugeridos, para posteriormente aclarar dudas en clase.
- El profesor explicará el material en clase y en ocaciones pedirá que algunos de los estudiantes prepare algunos resultados estándar para presentar en la clase.
- Trabajaremos también con base en un proyecto que se ira desarrollando en el semestre acádemico completo.

- **CONTENIDO DE LA ASIGNATURA**

  - **Números primos.**
    Un número primo es un número natural mayor que 1 que tiene únicamente dos divisores positivos distintos: él mismo y el 1. Los números primos son considerados los bloques fundamentales en la aritmética, pues según el teorema fundamental del álgebra cada número puede escribirse en fórma única como un producto de primos. En esta primera unidad veremos la demostración completa del teorema fundamental del álgebra, hablremos sobre la distribuciòn de los números primos y varios problemas abiertos de gran interés en el área.

  - **Aritmética modular**
    El anillo de los enteros módulo n, fue introducido por Carl Friedrich Gauss en su libro Disquisitiones Arithmeticae, publicado en 1801 y aún hoy en día juega un papel importante en la teoría de números, no sólo por los aspectos teorícos si no por sus aplicaciones a criptografía y seguridad informática. Desde un punto de vista teorico nos permitira resultados de los enteros como el Teorema Chino del resto y desarrollar algunas pruebas de primalidad. Por otro lado el grupo de unidades posteroriormente tendrá aplicaciones interesantes y por ello en este módulo investigaremos su estructura.

  - **Criptografía de llave pública**
    Un aspecto interesantísimo de la teoría de números es que esta esta presente en nuestras vidad diarias, cuando usamos el internet y enviamos información importante (tarjetas de crédito, passwords y otros). En este módulo veremos en detalle algunos conceptos e ida de criptografía que involucran la teoría de números y que se explican con los resultados de los dós módulos anteriores. Además veremos implementaciones en Sage (Python) de RSA.

  - **Reciprocidad cuadrática**
    La ley de la reciprocidad cuadrática es un teorema sobre aritmética modular que da condiciones para la solubilidad de ecuaciones cuadráticas módulo números primos.

César Galindo
Cn.galindo1116@uniandes.edu.co

El teorema de reciprocidad cuadrática fue conjeturado por Euler y Legendre y primero probado por Gauss, quien se refirió a él como el "teorema fundamental" en sus Disquisitiones Arithmeticae y sus artículos, escribiendo

"Sin duda, el teorema fundamental debe considerarse como uno de los más elegantes de su tipo."

En privado, Gauss se refirió a él como el "teorema dorado" Publicó seis pruebas del teorema, y se encontraron dos más en sus artículos póstumos. En la actualidad hay más de 240 pruebas publicadas. En este módulo presentaremos una demostración elegante que hace uso de la teoría de caracteres de grupos abelianos finitos un tema interesante por si mismo y con diversas aplicaciones.

- **CRONOGRAMA**

DEPARTAMENTO DE MATEMÁTICAS
PROGRAMA DEL CURSO MATE-XXXX
Primer semestre de 2021*

Semana No.	Mes	Fecha	Tema de clase
1	**Enero**	25 Lu	
		26 Ma	
		27 Mi	Introducción al curso
		28 Ju	
		29 Vi	Factorización y lo números primos
2	**Febrero**	1 Lu	
		2 Ma	
		3 Mi	Teorema fundamental de la aritmética
		4 Ju	
		5 Vi	La distribución de los números primos
3	**Febrero**	8 Lu	
		9 Ma	
		10 Mi	Congruencias módulo n
		11 Ju	
		12 Vi	El teorema chino del resto
4	**Febrero**	15 Lu	
		16 Ma	

César Galindo
Cn.galindo1116@uniandes.edu.co

		17 Mi	Cálculando inversos y pontencias grandes
		18 Ju	
		19 Vi	Pruebas de primalidad
5	**Febrero**	22 Lu	
		23 Ma	
		24 Mi	Repaso para le primer parcial
		25 Ju	
		26 Vi	**Parcial 1**
6	**Marzo**	1 Lu	
		2 Ma	
		3 Mi	La estructura de (Z/pZ)^*
		4 Ju	
		5 Vi	Introducción a la criptografía
7	**Marzo**	8 Lu	
		9 Ma	
		10 Mi	El sistema de intercambio de llaves de Diffie-Hellmande
		11 Ju	
		12 Vi	El criptositema RSA (primera parte)
8	**Marzo**	15 Lu	
		16 Ma	
		17 Mi	El criptositema RSA (segunda parte)
		18 Ju	
		19 Vi	Atacando RSA
Semana de receso –marzo 22 al 27			
Semana Santa – marzo 29 al 3 de abril.			
9	**Abril**	5 Lu	
		6 Ma	
		7 Mi	Repaso segundo parcial
		8 Ju	
		9 Vi	Último día para informar el 30% Segundo parcial
10	**Abril**	12 Lu	
		13 Ma	
		14 Mi	Introducción a la reciprocidad cuadrática
		15 Ju	

César Galindo
Cn.galindo1116@uniandes.edu.co

		16 Vi	El criterio de Euler
11	**Abril**	19 Lu	
		20 Ma	
		21 Mi	Caracteres de grupos abelianos
		22 Ju	
		23 Vi	Demostración de la reciprocidad cuadratica
12	**Abril**	26 Lu	
		27 Ma	
		28 Mi	Buscando raices cuadradas
		29 Ju	
		30 Vi	Introducción a las fracciones continuas
13	**Mayo**	3 Lu	
		4 Ma	
		5 Mi	Fracciones continuas infinitas
		6 Ju	
		7 Vi	La fracción continua de e
14	**Mayo**	10 Lu	
		11 Ma	
		12 Mi	Cuadraticos irracionales
		13 Ju	
		14 Vi	Suma de dos cuadrados
15	**Mayo**	17 Lu	*Festivo*
		18 Ma	
		19 Mi	Repaso
		20 Ju	
		21 Vi	Parcial
16	**Mayo**	24-29	
Exámenes finales – Mayo 31 a junio 5			
Último día para realizar retiros de materias: 15 de junio de 2021			

César Galindo
Cn.galindo1116@uniandes.edu.co

Recuerde el juramento del uniandino: "Juro solemnemente abstenerme de copiar o de incurrir en actos que pueden conducir a la trampa o al fraude en las pruebas académicas, o en cualquier otro acto que perjudique la integridad de mis compañeros o de la misma Universidad".

- **Bibliografía**

Libro de Guía:
Elementary Number Theory: Primes, Congruences, and Secrets. Undergraduate Texts in Mathematics, Springer-Verlag. 2008.

El libro puede descargarse en forma gratuita de la página web del autor. Haga click aquí para ir a la pagina de descarga.

Otros libros:

- Elementary Number Theory, 6th edition by Kenneth Rosen, Pearson. Se pidieron dos copias del libro a la biblioteca.
- Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. Wiley, 1991.
- Ireland, Kenneth F., and Michael I. Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 1990.
- Davenport, Harold, and James H. Davenport. *The Higher Arithmetic: An Introduction to the Theory of Numbers*. Cambridge University Press, 2008.

- **Criterios de evaluación y aspectos académicos**

✓ Porcentajes de cada evaluación
Parciales (tres parciales 10% cada uno) 30%
Tareas 30%
Proyecto (Escrito 20%, Presentación 15%,) 35%
Participación en clase (presentaciónes en clase) 5%

✓ Fechas Importantes
Primer parcial: 26 de febrero
Segundo parcial: 7 de abril
Tercer parcial: 21 de mayo

César Galindo
Cn.galindo1116@uniandes.edu.co

- ✓ Parámetros de calificación de actividades académicas
- ✓ Calificación de asistencia y/o participación en clase
- ✓ Reclamos
- ✓ Política de aproximación de notas

- **Calificación de asistencia y/o participación en clase:**

Se asignarán reularmente algunas mini exposiciones a los estudiantes para presentar en clase.

- **Reclamos**
  Si hay inconformidad por la nota asignada en una prueba, el estudiante deberá presentar su reclamo por escrito dentro del tiempo estipulado en el RGEPr (ver pág. 11).

- **Política de aproximación de notas**

Se acordarán con los estudiantes

RÉGIMEN ACADÉMICO

Las siguientes disposiciones académicas se deberán tener en cuenta en la elaboración de los programas de los cursos:

- **Asistencia a clase:**
  Los profesores iniciarán sus cursos desde el primer día del semestre académico, con la finalidad de garantizarles a los estudiantes el derecho a beneficiarse activa y plenamente del proceso educativo (Art. 40 RGEPr).
  Las clases de la Universidad deben empezar a la hora en punto o a la media hora, y terminar diez minutos antes de la hora en punto o de la media hora (Art. 41 RGEPr).

- **Inasistencia a clase y a evaluaciones:**

  Los parámetros para controlar la asistencia deberán ser informados a los estudiantes el primer día de clase. Se sugiere informar si la asistencia y la participación serán criterios de evaluación, así como la forma en que serán calificados. Será facultativo de cada profesor determinar las consecuencias de la inasistencia si esta supera el 20% (Art. 42 y 43 RGRPr).
  El estudiante que desee justificar su ausencia deberá hacerlo ante el profesor dentro de un término no superior a ocho (8) días hábiles siguientes a la fecha de ésta. De acuerdo con el parágrafo del artículo 45 del RGEPr, serán excusas válidas las siguientes:

César Galindo
Cn.galindo1116@uniandes.edu.co

a. Incapacidades médicas.
b. Incapacidades expedidas por la Decanatura de Estudiantes.
c. Muerte del cónyuge o de un familiar hasta del segundo grado de consanguinidad.
d. Autorización para participar en eventos deportivos, expedida por la Decanatura de Estudiantes.
e. Autorización para asistir a actividades académicas y culturales, expedida por la respectiva dependencia académica.
f. Citación a diligencias judiciales, debidamente respaldada por el documento respectivo.

El profesor podrá tener en cuenta otras circunstancias que a su criterio puedan justificar la ausencia del estudiante.
La Decanatura de Estudiantes prestará colaboración en la verificación de las incapacidades médicas.

- **Salidas de campo:**

Las salidas de campo de los estudiantes de la Universidad, programadas fuera de Bogotá, no son de carácter obligatorio. En caso de que algunos estudiantes no puedan cumplir con esta actividad, deberán informar las razones al profesor respectivo y acordar con él la realización de trabajos supletorios (Art. 46 RGEPr).

- **Calificaciones:**

  - Se deberán programar como mínimo tres (3) evaluaciones. En los cursos de la escuela de verano el profesor podrá practicar una sola evaluación con un valor equivalente al 100% de la materia (Art. 47 y parágrafo Art. 48 RGEPr).
  - Ninguna de las evaluaciones podrá tener un porcentaje superior al 35%, salvo que se trate de prácticas académicas, proyectos de grado, los cursos con formato de taller y algunos cursos del programa de música, los cuales tendrán un sistema de calificación especial que también deberá ser informado a los estudiantes en el programa del curso.
  - Las evaluaciones orales, en las que la actividad del estudiante consiste únicamente en responder las preguntas formuladas por el profesor y que tengan un valor superior al 15% de la calificación del curso, deberán realizarse en presencia de un profesor adicional, quien también deberá actuar como evaluador.
  - Si un estudiante falta a la presentación de una evaluación debidamente programada, podrá ser calificado con cero (0,0). Sin embargo, el estudiante podrá justificar su ausencia ante el profesor dentro de un término no superior a (8) días hábiles siguientes a la realización de la prueba. Justificada la inasistencia el profesor deberá indicarle al estudiante la nueva fecha y hora en que le realizará el examen, dentro de las dos (2) semanas siguientes a la aceptación de la justificación presentada.
  - El valor de cada evaluación practicada sin aviso, en ningún caso, podrá superar el 5% de la nota definitiva del curso.
  - Los profesores tendrán autonomía para establecer sus propios criterios de aproximación de notas definitivas, pero deberán siempre informarlo en el programa del curso, el primer día de clase.

César Galindo
Cn.galindo1116@uniandes.edu.co

- Se recomienda establecer desde un inicio las condiciones para la entrega de informes y trabajos, así como los parámetros para la elaboración las actividades en grupo. También indicar los efectos de la entrega tardía de trabajos y de la no entrega.

- **Entrega de calificaciones:**

  - Todos los profesores de la Universidad deben hacer conocer a sus estudiantes las calificaciones obtenidas, dentro de los diez (10) días hábiles siguientes a la práctica de la evaluación parcial. Exceptuando aquellas correspondientes a los proyectos de grado y prácticas académicas (Art. 68 RGEPr).
  - Al menos el 30% de las calificaciones debe ser publicado en el sistema banner, a más tardar antes de la semana de retiros de cada semestre (Art. 69 RGEPr).
  - Antes del examen final, el estudiante tiene el derecho a conocer las calificaciones parciales obtenidas durante el semestre y podrá solicitarlas al profesor (Art. 70 RGEPr).

- **Notas especiales:**

  - *Incompleto (I)*: nota aplicada por el Consejo de Facultad cuando el alumno no haya podido cumplir por razones justificadas, con los requisitos del curso (Art. 57 RGEPr).
  - *Incompleto Total (IT)*: nota aplicada por el Consejo de Facultad cuando el alumno no haya podido cumplir por razones justificadas, con los requisitos de todos los cursos del periodo académico en el cual se encuentra matriculado (Art. 58 RGEPr).
  - *Pendiente (P)*: nota aplicada por el profesor cuando al estudiante por razones de fuerza mayor, para cumplir con los requisitos del curso, solo le reste la presentación de una prueba final o no pueda asignársele una calificación antes del plazo determinado por la Dirección de Admisiones y Registro. La nota 'P' deberá reemplazarse a más tardar un mes después de terminado el semestre académico o quince (15) días después de terminado el periodo intersemestral (Art. 59 y Art. 60 RGEPr).
  - *Pendiente Disciplinario (PD)*: nota aplicada por el profesor al estudiante que se encuentre vinculado a un proceso disciplinario. Esa nota será reemplazada una vez culmine definitivamente el proceso (Art. 61 y parágrafo 1 Art. 115 RGEPr).
  - *Pendiente Especial (PE)*: nota excepcional aplicable a aquellos estudiantes que se encuentren desarrollando su correspondiente proyecto de grado y no ha sido concluido, por razones justificadas, dentro del semestre inicialmente establecido (Art. 63 RGEPr).

- **Reclamos:**

  Si se trata de una prueba escrita, el estudiante deberá dirigir el reclamo por escrito, dentro de los cuatro (4) días hábiles siguientes al que conoció la calificación en cuestión. El profesor cuenta con cinco (5) días hábiles para responderle. Si el estudiante considera que la decisión no corresponde a los criterios de evaluación, podrá solicitar la designación de un segundo calificador ante el Consejo de Facultad, dentro de los cuatro (4) días hábiles al conocimiento de la decisión (Art. 64 y 65 del RGEPr).

César Galindo
Cn.galindo1116@uniandes.edu.co

En caso de reclamo por una calificación obtenida en una prueba oral, el estudiante podrá exponer la razón de su desacuerdo a los profesores evaluadores en el mismo momento en que tiene conocimiento de la nota. Si el grupo evaluador mantiene la calificación, la realización de un nuevo examen quedará a discreción del Consejo de Facultad al que pertenece la materia, previa solicitud escrita del estudiante (Art. 66 del RGEPr).

- **Cambio de notas definitivas:**

  Vencido el plazo previsto para el cambio notas derivadas de los reclamos presentados, estos solo podrán realizarse con la autorización del coordinador de pregrado del programa al que pertenece la materia (Art. 67 RGEPr).

- **Funciones del monitor:**

  La principal función del monitor es la de ayudar al profesor en la dirección de las actividades académicas (laboratorios, sesiones de repaso o de ejercicios, asesoría a estudiantes). Así mismo, apoyarlo en la corrección de ejercicios y pruebas. La calificación definitiva de las pruebas será responsabilidad exclusiva del profesor.

- **Reporte de casos disciplinarios:**

  Ante la sospecha de una presunta comisión de fraude académico (Art. 115 RGEPr) o de una falta disciplinara (Art. 116 y 117 RGEPr) por parte de uno de sus estudiantes o de cualquier miembro de la comunidad uniandina, los profesores deberán tener en cuenta:

  - Es su deber informar al secretario del Comité Disciplinario de la facultad a la que pertenece el estudiante, mediante comunicación escrita que exprese de manera clara y sucinta los hechos. Se adjuntarán las pruebas correspondientes. (Art. 129 RGEPr).

  - A través de un proceso disciplinario el estudiante tendrá la oportunidad formal de presentar su versión sobre los hechos y pronunciarse sobre las decisiones que tomé el Comité (Art. 130 – 146 RGEPr).

  - El profesor tiene discreción para hablar con los estudiantes implicados antes de reportar el caso al comité, para informarles al respecto.

  - Durante el proceso disciplinario el profesor podrá ser consultado si el Comité lo considera, pero no será parte formal del proceso.

César Galindo
Cn.galindo1116@uniandes.edu.co

- A menos que el estudiante acepte su responsabilidad, el profesor no puede afirmar que cometió una falta disciplinaria. En cualquier conversación con un estudiante que presuntamente haya cometido la falta, el profesor debe ser cuidadoso. La existencia del fraude o de una falta disciplinaria solamente la puede determinar el Comité, después de haberse cumplido el proceso contemplado en los distintos reglamentos de estudiantes de la Universidad.

- La actividad académica en la que se presuma la comisión de un fraude académico deberá ser calificada con Pendiente Disciplinario (PD), (Art. 61 RGEPr). Es indispensable poner el Pendiente Disciplinario pues esta nota es una garantía del respeto por la presunción de inocencia del estudiante.

- Una vez el profesor reciba copia de la carta por medio de la cual se le notifica al estudiante la culminación del proceso disciplinario, deberá levantar el PD y asignar la nota correspondiente a la actividad académica (Art. 129 y parágrafo 2 Art. 129 RGEPr).

- **Canales de ayuda para estudiantes y profesores:**

  En cualquier momento los profesores y estudiantes podrán apoyarse en la labor de los coordinadores de su programa, la Decanatura de Estudiantes, la Secretaría General de la Universidad y la Oficina del Ombudsperson para consultar sobre asuntos académicos o administrativos según corresponda.

- **Ajustes razonables**

  Según el Art.2 de la Convención sobre los Derechos de las personas con discapacidad de la ONU, se entiende por ajustes razonables "las modificaciones y adaptaciones necesarias y adecuadas que no impongan una carga desproporcionada o indebida, cuando se requieran en un caso particular, para garantizar a las personas con discapacidad el goce o ejercicio, en igualdad de condiciones con las demás, de todos los derechos humanos y libertades fundamentales". Por lo tanto, siéntase en libertad de informar a su profesor lo antes posible si tiene alguna condición o situación de discapacidad, visible o invisible, y requiere de algún tipo de apoyo o ajuste para estar en igualdad de condiciones con los demás estudiantes. En caso dado, por favor justifique su solicitud con un certificado médico o constancia de su situación. Así mismo, lo invitamos a buscar asesoría y apoyo en la dirección de su programa, en la decanatura de Estudiantes (Bloque Ñf, ext.2330, http://centrodeconsejeria.uniandes.edu.co) o en el Programa de Acción por la Igualdad y la Inclusión Social (PAIIS) de la Facultad de Derecho (paiis@uniandes.edu.co).

- **Política de momentos difíciles -Nuevo**

Todas las personas pueden pasar por un momento difícil que de alguna manera pueda afectar nuestra vida en la Universidad. Pueden ser problemas en casa, con la pareja, incluso estrés por esta u otra materia. Si usted siente que está pasando por un momento complicado, sin importar el motivo, siéntase con la tranquilidad de hablar con el profesor para pedir tiempo o apoyo. Ningún trabajo o entrega puede sobrepasar su salud mental y física. Su bienestar es lo más importante.

César Galindo
Cn.galindo1116@uniandes.edu.co

- **Respeto por la diversidad**

  Los valores de inclusión y respeto por la diversidad son fundamentales para nuestra labor. En esta comunidad consideramos inaceptable cualquier situación de acoso, discriminación, matoneo, y/o amenaza. Si alguno de los miembros de esta comunidad siente que está pasando por alguna de estas situaciones o sabe de alguien a quien esto le puede estar pasando puede denunciar su ocurrencia y buscar orientación y apoyo ante alguna de las siguientes instancias:

  - el equipo pedagógico del curso o la dirección del programa,
  - la Decanatura de Estudiantes (DECA),
  - la Ombudsperson (ombudsperson@uniandes.edu.co).
  - el Comité MAAD (Maltrato, Acoso, Amenaza y Discriminación) (lineamaad@uniandes.edu.co, https://secretariageneral.uniandes.edu.co/index.php/es/inicio-es/14-noticias/128).

  También puede acudir a los representantes estudiantiles (CEU) y/o a los grupos estudiantiles que pueden prestarle apoyo y acompañamiento: No Es Normal (derechoygenero@uniandes.edu.co o https://www.facebook.com/noesnormaluniandes/?fref=ts); Pares de Acompañamiento Contra el Acoso (paca@uniandes.edu.co o https://www.facebook.com/PACA-1475960596003814/?fref=ts). Además, en clase usted podrá solicitar ser identificado con el nombre y los pronombres que usted prefiera, estos pueden coincidir o no con su nombre legal registrado en banner. No obstante, para firmar en listas de asistencia y marcar hojas de exámenes, debe usar su nombre legal.