Universidad de Costa Rica
Facultad de Ciencias
Escuela de Matemática

Carta al estudiante
Departamento de Educación Matemática
MA-0025 Teoría de Números
II-Ciclo 2020

Nivel de virtualidad del curso: Virtual	
Año: IV	**Requisitos:** MA-0009 y MA-0020
Ciclo: VIII	**Correquisitos:** Ninguno
Tipo de curso: Teórico	**Horas virtuales por semana:** 5
Créditos: 4	**Horas de trabajo independiente por semana:** 7

Profesor: Adrián Alberto Barquero Sánchez
email: adrianbs11@gmail.com o adrian.barquero_s@ucr.ac.cr
página web: https://sites.google.com/view/adrian-barquero-sanchez/home
Oficina: 327 Edificio Anexo de Matemáticas/CIMPA (Ciudad de la Investigación)
Horario de clases: Las clases virtuales sincrónicas serán grabadas y los videos se subirán al entorno del curso en Mediación Virtual.

- Lunes de 9:00 a 11:50 por videoconferencia de Zoom.
- Jueves de 9:00 a 10:50 por videoconferencia de Zoom.

Horas de Consulta: Por videoconferencia de Zoom: Miércoles 15:30 - 17:00 o por mensaje de texto por medio de WhatsApp.

Descripción del curso:

La Teoría de Números, que en un sentido muy superficial y sobre simplificado podría describirse como el estudio de propiedades de los números enteros, es una de las áreas más importantes de la matemática moderna, con aplicaciones fundamentales a distintas ramas, particularmente, a la transmisión de información en internet de manera segura, en la criptografía y la teoría de códigos. De hecho, en 1974, el famoso matemático y científico de la

computación, Donald Knuth (el creador del sistema de tipografía TEX), dijo que *"virtualmente todo teorema de la teoría elemental de números aparece de una manera motivada y natural en conección con el problema de hacer que las computadoras hagan cálculos numéricos a alta velocidad"*.
En este curso estudiaremos algunos de los temas más básicos de la Teoría de Números Elemental, como divisibilidad, congruencias, funciones aritméticas, aproximación diofántica básica (fracciones continuadas) y ecuaciones diofánticas. Adicionalmente, en el curso daremos una introducción a la criptografía de clave pública y a las firmas digitales.
También, daremos una introducción al uso del sistema algebraico computacional `SageMath` y lo utilizaremos como herramienta para realizar experimentos y cálculos numéricos con los objetos de estudio del curso.

Objetivos:

El objetivo principal del curso es introducir a los estudiantes a algunos de los temas y de las técnicas básicas de la Teoría de Números y sus aplicaciones a la criptografía y las firmas digitales, a un nivel elemental. Para esto, algunos de los objetivos específicos que se espera que el estudiante logre al finalizar el curso son los siguientes:

1. Realizar experimentos numéricos a mano y por computadora con los objetos de la Teoría de Números para aplicar los resultados de estos experimentos en su estudio.
2. Aplicar las definiciones y resultados básicos acerca de la divisibilidad en los números enteros para poder utilizarlos en la resolución de problemas de la teoría de números elemental.
3. Aplicar las definiciones y los teoremas básicos acerca de la teoría de congruencias para poder utilizarlos en la resolución de problemas de la teoría de números.
4. Aplicar las definiciones y resultados básicos sobre funciones aritméticas como la función φ de Euler y la función μ de Möbius para poder utilizarlos en la resolución de problemas que involucran su utilización.
5. Aplicar las definiciones y teoremas básicos sobre números algebraicos en cuerpos cuadráticos para poder aplicarlos en la resolución de problemas de la teoría elemental de números.
6. Aplicar las definiciones y teoremas básicos sobre sobre aproximación diofántica y fracciones continuadas para poder aplicarlos en la aproximación de números reales por números racionales.
7. Explicar algunas de las técnicas básicas utilizadas para la resolución de ecuaciones diofánticas para que el estudiante pueda tener una mejor perspectiva de la dificultad involucrada en el estudio de este tipo de problemas y para que pueda aplicarlas en la solución de algunas ecuaciones diofánticas básicas.
8. Aplicar los métodos básicos de la criptografía de clave pública para encriptar y decriptar mensajes sencillos.
9. Comprender los fundamentos matemáticos básicos de las firmas digitales para poder explicar esto como una aplicación muy importante de la Teoría de Números.

Contenidos:

La siguiente es una lista de los temas que estudiaremos en el curso. Se indica además el tiempo aproximado que esperamos dedicar a cada tema.

1. (1 semana) Introducción a la Teoría de Números y a `SageMath`.
2. (2 semanas) Divisibilidad y números primos: Definición y propiedades básicas de la divisibilidad. Máximo común y mínimo común múltiplo. Números primos y el Teorema Fundamental de la Aritmética. Ecuaciones diofánticas lineales.
3. (2 semanas) Congruencias: Definición de congruencia y clases residuales. El Teorema Pequeño de Fermat y el Teorema de Euler. Solución de ecuaciones con congruencias lineales. El Teorema Chino de los Residuos.
4. (2 semanas) Reciprocidad cuadrática: Congruencias cuadráticas y el símbolo de Legendre. El criterio de Euler. La Ley de la Reciprocidad Cuadrática. El símbolo de Jacobi.
5. (1 semana) Funciones aritméticas: Definición de función aritmética y ejemplos básicos.
6. (3 semanas) Criptografía y firmas digitales: Introducción a la criptografía de clave pública. Cifrados de sustitución. Cifrados simétricos y asimétricos y codificación de mensajes por medio de números. El problema del logaritmo discreto. El intercambio de claves de Diffie-Helmann y el sistema criptográfico de Elgamal. El criptosistema de clave pública RSA. Implementación y temas de seguridad. Introducción a las firmas digitales. Firmas digitales RSA.
7. (2 semanas) Fracciones continuadas: Definición de fracción continuada y ejemplos de cálculo. Fracciones continuadas finitas e infinitas. Aproximación de números reales por medio de racionales.
8. (2 semanas) Ecuaciones diofánticas: Ecuaciones diofánticas y congruencias, tripletas Pitagóricas y el Último Teorema de Fermat. La ecuación de Pell-Fermat.
9. (1 semana) Sumas de cuadrados: Los enteros Gaussianos y el Teorema de Fermat sobre sumas de dos cuadrados. El Teorema de Lagrange sobre sumas de cuatro cuadrados.

Metodología:

La modalidad del curso será virtual, por medio de clases sincrónicas a llevarse a cabo en el horario oficial del curso por medio de la plataforma Zoom. Estas clases serán grabadas y los videos se subirán al entorno del curso en Mediación Virtual. Durante el curso buscaremos abordar los cinco ejes de formación sobre los que se basa la carrera de Educación Matemática y la metodología que emplearemos en cada caso se detalla a continuación.

1. **Historia y epistemología de la matemática:** La Teoría de Números es junto con la Geometría Euclideana, la rama más antigua de la matemática. Durante el curso abordaremos muchos de los temas mencionando algunos de los desarrollos históricos más importantes y también hablaremos sobre algunos de los personajes más influyentes en el desarrollo de la Teoría de Números que estudiaremos.

2. **Didáctico-matemática:** Este eje de formación será abordado por medio de sesiones de ejercicios semanales en las que los estudiantes presentarán soluciones de ejercicios previamente asignados. Cada cierto tiempo tendremos un periodo de discusión crítica sobre las estrategias didácticas utilizadas por los estudiantes en la presentación de sus soluciones, así como una valoración sobre la aplicación o no de estos ejercicios en educación primaria o secundaria, adaptando el nivel de complejidad, o bien si los programas del Ministerio de Educación Pública proponen algún acercamiento a los temas en estudio.

3. **Desempeño profesional:** Este eje será abordado de forma conjunta con el anterior. Adicionalmente, como parte de la evaluación del curso, cada estudiante deberá realizar una clase de unos 50 minutos sobre un tema a escoger previamente en conjunto con el profesor. En particular, la clase puede ser sobre algún tema de teoría, una estrategia didáctica o una clase que relate el desarrollo histórico de algún tema particular en la Teoría de Números o de alguna de sus aplicaciones.

4. **Aplicaciones de la matemática:** Como es el común denominador con prácticamente todas las áreas de la matemática, la Teoría de Números tiene una enorme influencia a nivel de aplicaciones a la vida cotidiana. Una de las aplicaciones más importantes de la Teoría de Números es a la criptografía. Durante el curso daremos una introducción a la criptografía de clave pública y además a las firmas digitales, que tanta relevancia han tomado en estos últimos meses para el trabajo remoto.

5. **Tecnologías de la información y la comunicación (TIC):** Este eje será abordado por medio del uso extenso del Sistema Algebraico Computacional (CAS por sus siglas en inglés) `SageMath`. Este sistema nos permitirá no solo dar una introducción a la programación en Python (lenguaje en el que está programado `SageMath`), sino que también nos permitirá realizar diversos experimentos numéricos con los objetos de estudio de la Teoría de Números. De este modo el estudiante será capaz de experimentar y generar evidencia numérica para observar patrones y generar conjeturas, lo cual es parte fundamental de los métodos de investigación que han llevado a una enorme cantidad de descubrimientos en Teoría de Números.

Evaluación:

La evaluación del curso está dividida de acuerdo a la siguiente tabla.

Presentación de soluciones de ejercicios	20 %
Presentación de un tema	20 %
Tarea programada en `SageMath` I	10 %
Tarea programada en `SageMath` II	10 %
Examen oral I	20 %
Examen oral II	20 %

En las siguientes secciones se da una breve explicación sobre el Proyecto en LaTeX y los Proyectos de exploración y descubrimiento.

Calendario de evaluaciones

El siguiente es el calendario de evaluaciones del curso. Este puede estar sujeto a cambios por motivos de fuerza mayor. En caso de que esto ocurra, se avisaría oportunamente de tales cambios.

Evaluación	Día
Tarea programada en `SageMath` I	Jueves 1º de Octubre 2020
Tarea programada en `SageMath` II	Lunes 16 de Noviembre 2020
Examen Oral I	Miércoles 14 de Octubre 2020
Examen Oral II	Miércoles 2 de Diciembre 2020
Examen de Ampliación	Miércoles 9 de Diciembre 2020

Reporte de la nota final del curso N_{final} y examen de ampliación

La nota final del curso se determinará de acuerdo a la fórmula usual según se especifica en los artículos 25 y 28 del Reglamento de Régimen Académico Estudiantil de la Universidad de Costa Rica, como se describe a continuación.
La nota final del curso N_{final} se obtendrá a partir de la nota de aprovechamiento N_{aprov}, expresada en una escala de 0 a 10, redondeada a la unidad o media unidad más próxima. La nota final del curso N_{final} es la que se reportará a la Oficina de Registro e Información, salvo en el caso de que $N_{\text{final}} = 6{,}0$ o que $N_{\text{final}} = 6{,}5$, en cuyo caso el estudiante tiene derecho a realizar un exámen de ampliación, a realizarse en la fecha indicada en el calendario de exámenes del curso. Si el estudiante obtiene una nota igual o superior a 7.0 en la prueba de ampliación, la nota final que se le reportará en el curso será 7.0. Si la nota de la prueba de ampliación es estrictamente menor a 7.0, se reportará como nota de aprovechamiento un 6.0 o 6.5, según haya sido el caso.

Reposición de evaluaciones, trabajos y otras actividades de evaluación

Si un estudiante no puede realizar alguna de las evaluaciones del curso, la realización de su respectiva reposición está sujeta a lo dispuesto en el artículo 24 del Reglamento de Régimen Académico Estudiantil de la Universidad de Costa Rica[1], el cual citamos a continuación.

> **ARTÍCULO 24.** Cuando el estudiante se vea imposibilitado, por razones justificadas, para efectuar una evaluación en la fecha fijada, puede presentar una solicitud de reposición a más tardar en cinco días hábiles a partir del momento en que se reintegre normalmente a sus estudios. Esta solicitud debe presentarla ante el profesor que imparte el curso, adjuntando la documentación y las razones por las cuales no pudo efectuar la prueba, con el fin de que el profesor determine, en los tres días hábiles posteriores a la presentación de la solicitud, si procede una reposición. Si ésta procede, el profesor deberá fijar la fecha de reposición, la cual no podrá establecerse en un plazo menor de cinco días hábiles contados a partir del momento en que el estudiante se reintegre normalmente a sus estudios. Son

[1] Este reglamento se puede consultar en la página web http://www.cu.ucr.ac.cr/normativ/regimen_academico_estudiantil.pdf

justificaciones: la muerte de un pariente hasta de segundo grado, la enfermedad del estudiante u otra situación de fuerza mayor o caso fortuito. En caso de rechazo, esta decisión podrá ser apelada ante la dirección de la unidad académica en los cinco días hábiles posteriores a la notificación del rechazo, según lo establecido en este Reglamento.

Sobre el fraude en las evaluaciones

En caso de detectarse cualquier tipo de fraude en la realización y cumplimiento de los distintos rubros de evaluación del curso, se aplicará lo dictado para tales efectos en el Reglamento de Orden y Disciplina de los Estudiantes de la Universidad de Costa Rica, el cual puede ser consultado en la dirección web https://www.cu.ucr.ac.cr/normativ/orden_y_disciplina.pdf. En particular, recordamos los siguientes tipos de faltas indicados en ese reglamento en los artículos 4 y 5:

- **Faltas muy graves:**
  1. Hacerse suplantar o suplantar a otro en la realización de actividades que por su naturaleza debe ser realizada por el estudiante, ya sea prueba, examen, control de conocimientos o cualquier otra operación susceptible de ser evaluada.
  2. Apoderarse por cualquier medio fraudulento o por abuso de confianza del contenido de una prueba, examen o control de conocimiento, en beneficio propio o ajeno, antes de su realización; o una vez realizada la evaluación procurar la sustracción, alteración o destrucción de fórmulas, cuestionarios, notas o calificaciones, etc., en beneficio propio o ajeno.
  3. Plagiar, en todo o en parte, obras intelectuales de cualquier tipo.
  4. Presentar como propia una obra intelectual elaborada por otra u otras personas, para cumplir con los requisitos de cursos, trabajos finales de graduación o actividades académicas similares.
- **Faltas graves:**
  1. Procurarse por cualquier medio ilícito, en el momento de la realización de la prueba, examen o control de conocimientos, cualquier tipo de información utilizable para ese efecto o del mismo modo suministrar a otro dicha información.
  2. Copiar de otro estudiante tareas, informes de laboratorio, trabajos de investigación o de cualquier otro tipo de actividad académica.

Guía para las referencias: No usaremos un libro de texto específico, pero se recomienda consultar y leer de algunos de los libros de la bibliografía. Siempre es bueno conocer distintas referencias pues los diferentes enfoques que se encuentran ayudan a una mejor comprensión de los temas. En particular, recomendamos especialmente consultar por ejemplo los libros de Harold Stark [Sta78], Marty Erickson et. al [EVG16], James K. Strayer [Str94], Daniel E. Flath [Fla18], Benjamin Hutz [Hut18], George Andrews [And94], o el de Joseph Silverman [Sil12]. A un nivel más avanzado y cubriendo un rango aún más amplio de temas de la Teoría de Números se puede recomendar el excelente libro de Kenneth Ireland y Michael Rosen [IR90]. Para los temas de criptografía la referencia principal será el libro de Jeffrey Hoffstein, Jill Pipher y Joseph Silverman [HPS14]. También se recomienda el capítulo sobre criptografía del libro de William Stein [Ste09]. Adicionalmente, para aprender sobre el uso de `SageMath` recomendamos el libro de Gregory Bard traducido al español [Bar20] y el libro de Razvan Mezei [Mez16]. También, se recomienda leer el artículo de William Stein [Ste13][2]para aprender sobre la filosofía de `SageMath` y sobre su historia y su relación con otros sistemas CAS. Para temas de historia se puede consultar por ejemplo el libro de John Stillwell [Sti10] o el libro de I. G. Bashmakova [Bas97].

Referencias

[And94] George E. Andrews. *Number theory*. Dover Publications, Inc., New York, 1994. Corrected reprint of the 1971 original. ↑7

[Bar66] I. A. Barnett. Mathematical Education Notes: The Theory of Numbers as a Required Course in the College Curriculum for Majors. *Amer. Math. Monthly*, 73(9):1002–1004, 1966.

[Bar20] Gregory V. Bard. *Sage para estudiantes de pregrado*. online, 2020. Disponible en http://www.sage-para-estudiantes.com/. ↑7

[Bas97] I. G. Bashmakova. *Diophantus and Diophantine equations*, volume 20 of *The Dolciani Mathematical Expositions*. Mathematical Association of America, Washington, DC, 1997. Translated from the 1972 Russian original by Abe Shenitzer and updated by Joseph Silverman. ↑7

[Dav08] H. Davenport. *The higher arithmetic*. Cambridge University Press, Cambridge, eighth edition, 2008. An introduction to the theory of numbers, With editing and additional material by James H. Davenport.

[Due89] James Duemmel. The Teaching of Mathematics: From Calculus to Number Theory. *Amer. Math. Monthly*, 96(2):140–143, 1989.

[EVG16] Marty Erickson, Anthony Vazzana, and David Garth. *Introduction to number theory*. Textbooks in Mathematics. CRC Press, Boca Raton, FL, second edition, 2016. ↑7

[Fla18] Daniel E Flath. *Introduction to number theory*. American Mathematical Soc., 2018. ↑7

[2]Este artículo se puede encontrar en la página web del autor https://wstein.org/papers/focm11/focm11.pdf.

[HPS14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2014. ↑7

[Hut18] Benjamin Hutz. *An experimental introduction to number theory*, volume 31 of *Pure and Applied Undergraduate Texts*. American Mathematical Society, Providence, RI, 2018. ↑7

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. ↑7

[Mez16] Razvan A Mezei. *An introduction to SAGE programming*. Wiley Online Library, 2016. ↑7

[Sil12] Joseph H. Silverman. *A friendly introduction to number theory*. Pearson Education, fourth edition, 2012. ↑7

[Sta78] Harold M. Stark. *An introduction to number theory*. MIT Press, Cambridge, Mass.-London, 1978. ↑7

[Ste09] William Stein. *Elementary number theory: primes, congruences, and secrets*. Undergraduate Texts in Mathematics. Springer, New York, 2009. A computational approach. ↑7

[Ste13] William Stein. Sage: creating a viable free open source alternative to Magma, Maple, Mathematica, and MATLAB. In *Foundations of computational mathematics, Budapest 2011*, volume 403 of *London Math. Soc. Lecture Note Ser.*, pages 230–238. Cambridge Univ. Press, Cambridge, 2013. ↑7

[Sti10] John Stillwell. *Mathematics and its history*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2010. ↑7

[Str94] James K. Strayer. *Elementary number theory*. Waveland Press, 1994. ↑7