

Titulación: Licenciado en Ciencias Matemáticas			
Departamento: Geometría y Topología			
Nombre de asignatura: Teoría Elemental de Números		Código: 214	Tipo: Optativa
Nivel 1 ^{er} ciclo	Curso	Semestre Segundo	Créditos ECTS: 7.5
Horas semanales: 5		Teoría: 3	Prácticas: 2
Nombre del profesor/es que imparte/n la asignatura: Celia Martínez Ontalba			
Objetivos: Conocer los problemas y resultados clásicos de la teoría elemental de números. Familiarizarse con sus demostraciones. Conocer algunos problemas abiertos y aplicaciones de la teoría de números.			
Competencias o destrezas que se van a adquirir: Conocimiento y comprensión de los temas recogidos en el apartado de contenido de la asignatura. Soltura en la resolución de problemas teórico-prácticos relativos a dichos temas.			
Prerrequisitos para cursar la asignatura: Ninguno.			
Contenido:			
<ol style="list-style-type: none"> 1. Divisibilidad en los números enteros; algoritmo de la división. Máximo común divisor y mínimo común múltiplo. El algoritmo euclídeo. La ecuación diofántica lineal $ax+by=c$. Numeración en base b. 2. Números primos. Teorema fundamental de la Aritmética. La criba de Eratóstenes. Teorema de Euclides. Algunos resultados y conjeturas sobre números primos y su distribución. 3. Congruencias; propiedades básicas. Criterios de divisibilidad. Congruencias lineales en una variable. Teorema chino del resto. Teorema de Wilson. Teorema de Fermat. Teorema de Euler. 4. Funciones aritméticas: definición y ejemplos, funciones aritméticas multiplicativas, convolución de funciones aritméticas. La función μ de Möbius; fórmula de inversión. La función ϕ de Euler. Las funciones τ y σ. Números perfectos. Aplicación a la criptografía: sistema RSA. 5. Restos cuadráticos. El símbolo de Legendre. Los símbolos de Legendre $(-1/p)$ y $(2/p)$. Ley de reciprocidad cuadrática. Congruencias cuadráticas en una variable. 6. Orden de un entero módulo n; raíces primitivas. Raíces primitivas para primos. Teorema de la raíz primitiva. Índices. Restos de potencias k-ésimas módulo n. 7. Ecuaciones diofánticas lineales. Ecuaciones diofánticas no lineales. La ecuación diofántica $x^2 + y^2 = z^2$; ternas pitagóricas. La ecuación diofántica $x^4 + y^4 = z^4$; método del descenso de Fermat. El último teorema de Fermat: principales hitos en su demostración. 8. Representación de números naturales como suma de dos cuadrados. Representación de números naturales como suma de más de dos cuadrados. Teorema de Lagrange. Sumas de potencias superiores. El problema de Waring. 9. Fracciones continuas finitas. Fracciones continuas infinitas. Representación de números reales mediante fracciones continuas. Fracciones continuas periódicas. La ecuación de Pell. 			

Bibliografía básica recomendada:

1. Burton, D. M., "Elementary Number Theory", Mc Graw-Hill, 2005.
2. Rosen, K. H., "Elementary Number Theory and its Applications", Pearson/Addison-Wesley, 5ª ed., 2005 (también sirven las ediciones 3ª y 4ª).
3. Strayer, J. K., "Elementary Number Theory", PWS Publishing Company, 1994.
4. Jones, G. A., Jones, J. M., "Elementary Number Theory", Springer, 1999.
5. Niven, I., Zuckerman, H. S., Montgomery, H. L., "An Introduction to the Theory of Numbers", John Wiley & Sons, 1991.

Método docente: Clases teóricas y prácticas participativas.**Tipo de evaluación:**

Exámenes finales en las convocatorias oficiales.

La participación en clase se valorará con hasta 2 puntos que se sumarán a la calificación del examen en la convocatoria de junio. En la convocatoria de septiembre la calificación será la del examen únicamente.

Idioma en que se imparte: Castellano.**Más información:** La contenida en el Campus Virtual

Madrid, 5 de junio de 2009

La Profesora:

Aprobado el

por el Consejo de Departamento.

El Director del Departamento:

Fdo.: Celia Martínez Ontalba

Fdo.: Jesús M. Ruiz