**Propuesta de Trabajo Fin de Grado en Matemáticas (curso 2021-2022)**

| |
|---|
| *Responsable de tutorización:* Pedro A. García Sánchez<br>*Departamento:* Álgebra<br>*Correo electrónico:* pedro@ugr.es |
| *Responsable de cotutorización:*<br>*Departamento:*<br>*Correo electrónico:* |
| *(Rellenar sólo en caso de que la propuesta esté realizada a través de un estudiante)*<br>*Estudiante que propone el trabajo:* Adrián González Gutiérrez |

| |
|---|
| *Título del trabajo:* Factorización y pruebas de primalidad de enteros |
| *Tipología del trabajo (marcar una o varias de las siguientes casillas):*<br><br>☒ Complementario de profundización<br>☐ Divulgación de las Matemáticas<br>☐ Docencia e innovación<br>☒ Herramientas informáticas<br>☐ Iniciación a la investigación |
| *Materias del grado relacionadas con el trabajo:* Informática I y II, Probabilidad, Álgebra I, II y III, Teoría de números y criptografía |
| *Descripción y resumen de contenidos:*<br><br>La factorización de enteros es un problema difícil de resolver para enteros “grandes”, y que tiene varias aplicaciones en Criptografía. De igual forma, determinar si un entero es o no primo es una tarea que puede ser bastante complicada. Para solventar este problema, existen varios pruebas de primalidad probabilísticas, que se basan en aritmética modular, probabilidad y teoría de números.<br><br>Se pretende en este trabajo estudiar tanto los procedimientos “clásicos” de factorización como las pruebas de primalidad. Al final del trabajo se mostrarán algunas aplicaciones en Criptografía. |
| *Actividades a desarrollar:*<br><br>- Estudio de métodos de factorización de enteros.<br>- Estudio de pruebas de primalidad tanto deterministas como probabilísticos.<br>- Estudio de aplicaciones en Criptografía. |

| *Objetivos matemáticos planteados* |
|---|
| - Comprensión y prueba formal del funcionamiento correcto de los algoritmos estudiados. |
| - Estudio de las distintas herramientas matemáticas que dan lugar a las distintas aproximaciones para la resolución del problema de factorización o de pruebas de primalidad. |
| - Estudio de las aplicaciones Criptográficas y de su corrección. |

*Bibliografía para el desarrollo matemático de la propuesta:*


- R. Guy, Pseudoprimes. Euler Pseudoprimes. Strong Pseudoprimes, §A12 in Unsolved Problems in Number Theory. 2nd ed., p. 28, New York: Springer-Verlag, 1994.
- N. Koblitz, A course in Number Theory and Cryptography, Springer, 1994.
- A. G. Konheim, Computer Security and Cryptography, Wiley, 2007
- V. Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press, 2008.
- S. Y. Yang, Number theory for computing, Springer, 2002


Firma del estudiante
(solo para trabajos propuestos por estudiantes)

Firma del responsable de tutorización
(solo para trabajos propuestos por estudiantes)

Firmado digitalmente por GARCIA SANCHEZ PEDRO ABELARDO - 24245401C
Fecha: 2021.05.26 '20:51:44 +02'00

En, Granada, a de de 2021