EMENTA

Introdução a Teoria dos Números, Estruturas Algébricas Finitas, Teoria dos Grafos e suas Aplicações.

CONTEÚDO PROGRAMÁTICO

01. Primos de Fermat e Mersenne.
02. Congruências Lineares, o Teorema Chinês dos Restos.
03. Os Teoremas de Fermat e Euler, Resíduos Quadráticos.
04. Funções Inteiras, as Funções de Euler e Möbius.
05. Introdução a Criptografia Moderna, o Criptossistema RSA.
06. Raízes Primitivas, o Sistema Diffie-Hellman.
07. Logaritmos Discretos, Criptografia baseada em Curvas Elípticas.
08. Grupos Finitos.
09. Anéis, Ideais e Domínios de Integridade.
10. Corpos Finitos.
11. Classes Ciclotômicas, Raízes e Fatoração de Polinômios.
12. Sequências de Comprimento Máximo.
13. Introdução a Teoria de Grafos.

BIBLIOGRAFIA

01. I. Niven, H. S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers, John Wiley, 5a. edição, 1991.
02. D.M. Burton, Elementary Number Theory, 7a. edição, McGraw-Hill, 2010.
03. W. Stallings, Criptografia e Segurança de Redes, Pearson Prentice-Hall, 2007.
04. J.H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, 2010.
05. M. Rosing, Implementing Elliptic Curve Cryptography, Manning Publications, 1999.
06. J. A. Gallian, Contemporary Abstract Algebra, 8a. edição, Cengage Learning, 2012.
07. J. R. Durbin, Modern Algebra: An Introduction, 6a. edição, Wiley, 2008.
08. R.J. McEliece, Finite Fields For Computer Scientists and Engineers, Kluwer, 1987.
09. R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2a. edição, 2008.

10. R.M. Campello de Souza, Matemática Discreta, Notas de Aula, DES-UFPE, 2012.
11. E. R. Scheinerman, Mathematics: A Discrete Introduction!, 3a. edição, Cengage Learning, 2012.