UNIVERSIDADE FEDERAL DE JUIZ DE FORA

INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
Tel: (32)3229-3308 – Fax: (32)3229-3315
E-mail: depto.mat@ufjf.edu.br

Disciplina: Introdução à Teoria dos Números
Código: MAT143
Pré-Requisitos: Não há.

Número de Créditos: 04
Carga Horária Semanal: 04 horas-aula
Carga Horária: 60 horas-aula

Ementa:

1- Os Princípios de Indução Matemática e da Boa Ordenação

2- Divisibilidade

3- Números Primos e o Teorema Fundamental da Aritmética

4- Equações Diofantinas Lineares

5- Congruências

6- Sistema de Congruências Lineares

7- Criptografia Básica

Bibliografia:

ALENCAR FILHO, E. **Teoria Elementar dos Números**. Livraria Nobel S.A., 1985.

FERNANDES, Â.M.V. e outros. **Fundamentos de Álgebra**. Editora UFMG, 2005.

SANTOS, J.P.O. **Introdução à Teoria dos Números**. Coleção Matemática Universitária. IMPA, 1998.

SHOKRANIAN, S. **Teoria dos Números**. Editora Universidade de Brasília, 1999.

GONÇALVES, A. **Introdução à Álgebra**. Projeto Euclides. IMPA, 1979.

DOMINGUES, H. H. & IEZZI, G. **Álgebra Moderna**. Atual Editora, 1982.

HEFEZ, A. **Curso de Álgebra**. Vol.1. Coleção Matemática Universitária. IMPA, 1993.

COUTINHO, S.C. **Números Inteiros e Criptografia RSA**. Série de Computação e Matemática. IMPA, 1997.

MILIES, F.C.P. **Números: Uma Introdução à Matemática**. Editora da Universidade de São Paulo, 2003.

HEFEZ, A. **Elementos de Aritmética**. Coleção Textos Universitários. SBM, 2005.

KOBLITZ, N. **A Course in Number Theory and Cryptography**. Springer-Verlag, 1987.

Programa Discriminado em Unidades e Sub-unidades:

1- OS PRINCÍPIOS DE INDUÇÃO MATEMÁTICA E DA BOA ORDENAÇÃO
Introdução. Dedução e Indução. Primeira Forma do Princípio de Indução. Segunda Forma do Princípio de Indução. Princípio da Boa Ordenação.

2- DIVISIBILIDADE
Relação de Divisibilidade em Z. Algoritmo da Divisão. Sistemas de Numeração. Critérios de Divisibilidade. Máximo Divisor Comum. Algoritmo de Euclides. Mínimo Múltiplo Comum.

3- NÚMEROS PRIMOS E O TEOREMA FUNDAMENTAL DA ARITMÉTICA
Números Primos e Compostos. Crivo de Eratósthenes. Teorema Fundamental da Aritmética. Números de Mersenne e Números de Fermat.

4- EQUAÇÕES DIOFANTINAS LINEARES
Definição e Exemplos. Condição de Existência de Solução. Soluções da Equação: $ax + by = c$.

5- CONGRUÊNCIAS
Inteiros Congruentes. Caracterização de Inteiros Congruentes. Propriedades das Congruências. Sistemas Completos de Resíduos. Classes Residuais módulo m e o Conjunto Z_m. Operações em Z_m. Congruências Lineares. Resolução de Equações Diofantinas Lineares por Congruência. Critérios de Divisibilidade usando Congruências. Teoremas de Fermat e de Wilson. A Função ϕ de Euler e o Teorema de Euler.

6- SISTEMA DE CONGRUÊNCIAS LINEARES
Introdução. Teorema do Resto Chinês. Representação Gráfica (tabela).

7- CRIPTOGRAFIA BÁSICA
Criptografia de Chave Pública: Sistema RSA.

Implantação: Segundo Semestre Letivo de 2009.