Ministério da Educação
Universidade Federal de São Paulo
Instituto de Ciência e Tecnologia

Plano de Atividades Domiciliares ADE

Unidade Curricular: Teoria dos Números e Criptografia

Professor: Grasiele Cristiane Jorge		**Contato:** grasiele.jorge@unifesp.br
Ano Letivo: 2021	**Semestre:** 1º	**Carga horária total:** 72h
Turma: I		
Plataforma de acesso ao curso: Google Classroom: http://classroom.google.com/		

Objetivos (remoto): Familiarizar o(a)s aluno(a)s com conceitos básicos de Teoria dos Números de forma que ele(a)s sejam capazes de reconhecer e resolver problemas relacionados aos números inteiros e suas propriedades básicas. Introduzir os conceitos de criptografia fazendo a relação entre a base matemática teórica com a parte computacional necessária para implementações numéricas. Discutir sobre a necessidade da sociedade contemporânea de proteção de dados. Compreender os aspectos interdisciplinares de Matemática, Computação e Humanidades, envolvidos no assunto e ter uma visão maior de como fazer relações semelhantes com outros temas estudados no curso.

Conteúdo Programático e Cronograma:

Semana	Conteúdo	CH síncrona*	CH assíncrona**
13/04-20/04	Divisibilidade nos inteiros e o algoritmo euclidiano da divisão	2h	2h
21/04-27/04	Máximo divisor comum, mínimo múltiplo comum e o algoritmo de Euclides	2h	2h
28/04-04/05	Números primos e Teorema Fundamental da Aritmética	2h	2h
05/05-11/05	Números especiais	2h	2h

Av. Cesare Mansueto Giulio Lattes, 1201. Parque Tecnológico.
Eugênio de Melo – CEP: 12247-014 – São José dos Campos, SP
Telefone: (12) 3924-9503 / 9547

12/05-18/05	Congruência	2h	2h
19/05-25/05	Divisibilidade	2h	2h
26/05-01/06	Equações diofantinas e congruência linear	2h	2h
02/06-08/06	Teorema de Wilson e Teorema de Fermat	2h	2h
09/06-15/06	A função fi de Euler, Teorema de Euler e Teorema Chinês dos Restos	2h	2h
16/06-29/06***	Funções Aritméticas	2h	6h
30/06-06/07	Raízes primitivas	2h	2h
07/07-13/07	Raízes primitivas (continuação)	2h	2h
14/07-20/07	Testes de primalidade	2h	2h
21/07-27/07	Testes de primalidade (continuação)	2h	2h
28/07-03/08	Criptografia e o Criptossistema RSA	2h	2h
04/08-10/08	O logaritmo discreto e o Criptossistema ElGamal	2h	2h
11/08-17/08	Criptografia pós-quântica	2h	2h

* encontros gravados via Google Meet para explicação do conteúdo semanal, resolução de exercícios e dúvidas.

** leitura de livros e notas de aula, visualização de vídeos, resolução de exercícios e atividades.

*** Congresso Acadêmico da Unifesp

Metodologia de Ensino Utilizada: Leitura de livros e notas de aula, visualização de vídeos, resolução de exercícios e atividades, participação em encontros via Google Meet para explicação do conteúdo semanal, resolução de exercícios e dúvidas (serão gravados e disponibilizados).

Metodologia de Avaliação: Atividades avaliativas assíncronas (AVAs) semanais. Um(a) aluno(a) obterá o conceito *cumprido* caso: realize ao menos 75% das AVAs e atinja um aproveitamento médio ponderado (AMP) maior ou igual a 60%. Caso contrário, ele(a) obterá o conceito *não-cumprido*. Para calcular este AMP, primeiro, denote os aproveitamentos dos(as) alunos(as), nas respectivas AVAs semanais da seguinte forma:

- AVA da semana 1: T1
- AVA da semana 2: T2
- AVA da semana 3: T3
- AVA da semana 4: T4
- AVA da semana 5: T5
- AVA da semana 6: T6
- AVA da semana 7: T7
- AVA da semana 8: T8
- AVA da semana 9: T9
- AVA da semana 10: T10
- AVA da semana 11: T11
- AVA da semana 12: T12
- AVA da semana 13: T13
- AVA da semana 14: T14
- AVA da semana 15: T15
- AVA da semana 16: T16
- AVA da semana 17: T17

Assim, o AMP será calculado da seguinte forma:

$$AMP = 0{,}7*((T4+T8+T12+T16)/4) + 0{,}3*((T1+T2+T3+T5+T6+T7+T9+T10+T11+T13+T14+T15+T17)/13).$$

Bibliografia básica e complementar para uso remoto:

- DA SILVA, R., *Teoria dos Números e Criptografia*, Arquivo disponibilizado aos discentes via Google Classroom.
- BURTON, D. M., *Teoria Elementar dos Números*, 7ª edição, LTC, 2016. Disponível em Minha Biblioteca/UNIFESP.
- HEFEZ, A., *Iniciação à Aritmética*, 2015. Disponível em http://www.obmep.org.br/docs/apostila1.pdf
- COUTINHO, S. C., *Criptografia*, 2015. Disponível em http://www.obmep.org.br/docs/apostila7.pdf
- DE MELO, L. A. C. P., Decifrando a Aritmética para o Ensino Fundamental, Dissertação de Mestrado, ICT-UNIFESP, 2017. Disponível em https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?cpf=37149561829&d=20210311104239&h=1511459becb60e8a48ea0210382ff4e298d38b42
- RIBEIRO, H. A., Raízes primitivas e aplicações em Criptografia, Dissertação de Mestrado, ICT-UNIFESP, 2018. Disponível em https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?cpf=36833802840&d=20210311104419&h=9f07059292986588d89483b64ddb48eb6bbb41a5