

Textos alternativos

Alguém perguntou sobre textos alternativos, além do citado na ementa, que é [SDK15]. (como falei, sugiro usar a versão original em inglês [SDK11] pois a tradução é horrível... lembre de consultar a errata do livro na minha página). A vantagem deste livro é que a ementa foi feita em cima dele, então é basicamente os primeiros 4 capítulos dele.

Na ementa que está no Jupiterweb, cita também GERSTING, e MENEZES, mas estes não conheço e não usei para preparar as aulas: pode dar uma olhada e eventualmente me falam se acharam bons.

Um livro que estava na antiga ementa é [GKP94]: lá podem achar alguns dos assuntos.

Para a parte de Teoria dos números e RSA usei bastante [Cou99, Cou00] (neste caso a versão original é a em português, mas eu só tenho a inglês).

Para a parte de contagem e de recorrências podem ver também as notas de aula ICMC que estão na minha página

Enfim, na minha página tem as minhas notas de 2021 (mas falta a parte recorrências).

Referências

- [Cou99] S. C. Coutinho, *The mathematics of ciphers*, A K Peters, Ltd., Natick, MA, 1999, Number theory and RSA cryptography, Translated and revised from the 1997 Portuguese original.
- [Cou00] S. C. Coutinho, *Números inteiros e criptografia RSA*, second ed., Série de Computação e Matemática [Computer and Mathematics Series], vol. 2, Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro; Sociedade Brasileira de Matemática, Rio de Janeiro, 2000.
- [GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994, A foundation for computer science.
- [SDK11] C STEIN, R DRYSDALE, and BOGART K., *Discrete mathematics for computer scientists.*, 1st edition ed., Pearson, 2011.
- [SDK15] C STEIN, R DRYSDALE, and BOGART K., *Matemática discreta - para ciência da computação.*, 1ª edição ed., Pearson, 2015.