Lectures Syllabus - 236315 Winter 2017/18
Exam A - 11/2/2018
Exam B - 11/3/2018

1. Intro, Karatsuba multiplication, Toom-Cook, Matrix multiplication
    a. http://alg15.cs.uchicago.edu/Handouts/karatsuba.pdf
    b. http://alg15.cs.uchicago.edu/Handouts/recurrence.pdf
    c. https://en.wikipedia.org/wiki/Toom%E2%80%93Cook_multiplication
    d. http://www.cs.ru/personal/karatsuba/divcen.pdf
    e. https://en.wikipedia.org/wiki/Strassen_algorithm
2. Fast Fourier transform,
    a. http://people.mpi-inf.mpg.de/~csaha/lectures/lec4.pdf
    b. http://www.cs.columbia.edu/~stratos/research/fft.pdf
    c. Google search “Fast Fourier Transform (Algorithm)” and “Discrete Fourier Transform (Algorithm)” and references therein
    d. An advanced mathematical discussion of the Fourier Transform: https://terrytao.wordpress.com/2009/04/06/the-fourier-transform/
3. Integer multiplication using FFT
    a. http://people.mpi-inf.mpg.de/~csaha/lectures/lec5.pdf
    b. http://www.cs.rug.nl/~ando/pdfs/Ando_Emerencia_multiplying_huge_integers_using_fourier_transforms_paper.pdf
4. the Fourier basis, Characters, Fourier analysis of the boolean cube
    a. https://lucatrevisan.wordpress.com/2011/01/28/cs359g-lecture-5-characters-of-abelian-groups/
    b. First 6 pages of http://theoryofcomputing.org/articles/gs001/gs001.pdf
    c. http://www.cs.huji.ac.il/~analyt/scribes/L07.pdf
5. Number Theory uses: Euclid’s GCD algorithm, Pattern matching, Diffie Hellman (DH), Discrete Log Problem (DLP), RSA
    a. Wikipedia and google search ...
6. Primality testing- Miller Rabin randomized test
    a. http://www.cs.cornell.edu/courses/cs482/2008sp/handouts/mrpt.pdf
7. The Agarwal-Kayal-Saxena (AKS) algorithm: “Primes is in P” (algorithm only)
    a. https://terrytao.wordpress.com/2009/08/11/the-aks-primality-test/
    b. https://www.cs.auckland.ac.nz/~msta039/primality_v6.pdf
    c. Lectures 11-13 from http://www.cs.technion.ac.il/~eli/courses/2010_Spring/notes_2010_Spring.pdf
8. Reed Solomon codes - Berlekamp Welch unique neighbor decoding
    a. https://en.wikipedia.org/wiki/Berlekamp%E2%80%93Welch_algorithm
    b. http://people.csail.mit.edu/madhu/FT02/scribe/lect11.pdf
    c. http://www.cse.buffalo.edu/faculty/atri/courses/coding-theory/lectures/lect27.pdf
9. Reed Solomon list decoding - Guruswami Sudan list decoding
    a. https://en.wikipedia.org/wiki/List_decoding
    b. http://www.cs.berkeley.edu/~luca/cs294/ - lecture 6
    c. http://people.csail.mit.edu/madhu/FT01/ - lecture 12
    d. http://madhu.seas.harvard.edu/talks/2009/TAMU-List.pdf