# Department of Information Technology, NITK

## Design and Analysis of Algorithms (IT257) - Laboratory Exercise 4
March 2023

1. Assume we have 8 numbers $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4$ and we consider these seven expressions. $p_1 = (a_1 + a_4)(b_1 + b_4), p2 = (a_3 + a_4)b_1, p_3 = a_1(b_2 - b_4), p_4 = a_4(b_3 - b_1), p_5 = (a_1 + a_2)b_4, p_6 = (a_3 - a_1)(b_1 + b_2), p_7 = (a_2 - a_4)(b_3 + b_4)$ Compute the following four sums.
$p_1 + p_4 - p_5 + p_7,\ p_3 + p_5,\ p_2 + p_4,\ p_1 - p_2 + p_3 + p_6$

   Now, apply divide and conquer technique to matrix multiplication. Let A and B be two n × n matrices, and we want to compute their product $C = AB$. The naive algorithm for this will take $O(n^3)$ arithmetic operations. We want to improve this using divide and conquer significantly. A natural way to split any matrix can be this:

$$\mathrm{A} = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$$

   where each $A_i$ is an n/2 × n/2 matrix.
   Express the product matrix C, in terms of $A_1, A_2, A_3, A_4$ and $B_1, B_2, B_3, B_4$.
   (c) Design an algorithm for matrix multiplication using divide and conquer which takes $\mathrm{O}(7^{log_2 n}) = \mathrm{O}(n^{log_2 7}) = \mathrm{O}(n^{2.81})$ time.
   ( Note: Refer https://36-750.github.io/algorithms/divide-conquer/ )

2. There is a resource that n people share. We want the resource to be accessible if and only if at least k out of the n people come together to access it. Can you devise a scheme to distribute the password/secret key that achieves this?
   (Hint: different representations of a polynomial.)

3. Write a program to find the square of an n-bit integer, using a squaring subroutine on five n/3-bit integers and a few additions/subtractions. Display the running time achieved for the devised algorithm.