JACOB MULHOLLAND

STUDENT, MATHEMATICS

THE LLL-ALGORITHM

“Let x1,x2 , . . . , xn be a basis of lattice L, and let æ(1/4 ,1) be a reduction parameter. The The Lenstra-Lenstra-Lovász Algorithm, or the LLL-Algorithm, can be used to find an α-reduced basis of L. In this talk, we will discuss the conditions required for a basis to be α-reduced. Then I will present the LLL-Algorithm into further detail. To conclude, an example of the algorithm will be presented.”

Research Advisor: Dr. Ha Tran