

Sonlu Cisimler Üzerinde Tanımlanan Permütasyon Polinomları

Bu konuşmamızda sonlu cisimler üzerinde tanımlanan permütasyon polinomlarından bahsedeceğiz. Sonlu bir cisim üzerinde tanımlanmış rastgele bir permütasyon polinomu bulmak aslında oldukça kolaydır ancak bizim amacımız olabildiğince basit formda ve bu polinomların uygulamaları için uygun olan permütasyon polinomları bulmak ve bu bir hayli zor olabilmektedir. Bu tür permütasyon polinomlarının kodlama teorisi, kriptografi ve benzeri alanlarda çok sayıda uygulaması bulunmaktadır. Konuşmamızda öncelikle gerekli temel tanım ve teoremlerden bahsederek daha sonra da bugüne kadar çeşitli matematikçilerle beraber bu konuda elde ettiğimiz sonuçları anlatmaya çalışacağız.