Abstract

We define a function which takes a polynomial with coefficients from the integers modulo a prime number and sends it to another polynomial with coefficients from the integers modulo the same prime number. Our main focus is to find the inverse to the function. We will see that the function is linear and so we can represent it as a matrix. Our problem then becomes to find the inverse to the matrix representation. We then start to study, and investigate, the fixed points but also how many times we have to apply the function to an element until we can be certain that we are back at the same element we started at.