***Galois Field Matrix’s Eigenvectors***

Author : HyeongRae Jo

Theorem : In Galois Field, invertible A is diagonalizable if, and only if A^(p-1) = I.

Proof :

If A is diagonalizable, A = SDS^(-1).

A^(p-1) = SD^(p-1)S^(-1) = SIS^(-1) = I.

This is because D^(p-1) is I. Eigenvalues of A are non-zero since A is invertible.

if A^(p-1) = I, A^(p-1) - I = 0.

Let p(x) = x^(p-1) - 1. This polynomial can annihilate A, meaning minimal polynomial mA(x) can divide it.

p(x) is 0 when x is 1,2, ~ , p-1, so p(x) can be rewritten to (x-1)(x-2)(x-3) ~ (x-(p-1)).

Since mA(x) can divide p(x), we know that mA(x) cannot have multiplicity more than 1, because p(x)’s multiplicities of all roots are all 1, meaning A is diagonalizable.