Even and odd nature for Pseudo τ-adic Non-Adjacent form

ABSTRACT

An algorithm was developed by previous researcher for elliptic scalar multiplication (SM) on Koblitz curve where the multiplier of SM is in the form of Pseudo -adic Non-Adjacent (pseudoTNAF). PseudoTNAF of an element of the ring Z) where is an expansion where the digits are generated by successively dividing by , allowing remainders of , 0 or 1. Such a multiplier is in the form of . In this paper, we refine some properties of the multiplier from previous researchers focusing on even and odd situation for and . We also propose two properties of when is even and is odd. As a result, the nature of and are depends on the nature of and when is even. Whereas, the nature of and are not depends on the nature of and when is odd.

Keyword: Pseudo -adic Non-Adjacent Form (pseudoTNAF); Scalar multiplication (SM); Koblitz curve