On some specific patterns of τ-Adic non-adjacent form expansion over ring Z (τ)

ABSTRACT

Let $\tau=(-1)^{1-a}+\sqrt{-7}/2$ for $a\in\{0, 1\}$ is Frobenius map from the set $E_a(F_2m)$ to it self for a point (x, y) on Koblitz curves E_a. Let P and Q be two points on this curves. τ-adic Non-Adjacent Form (TNAF) of α an element of the ring $Z(\tau) = \{\alpha = c+d\tau|c, d\in Z\}$ is an expansion where the digits are generated by successively dividing α by τ, allowing remainders of -1, 0 or 1. The implementation of TNAF as the multiplier of scalar multiplication nP = Q is one of the technique in elliptical curve cryptography. In this study, we find the formulas for TNAF that have specific patterns $[0, c_1, \ldots, c_{1-1}]$, $[-1, c_1, \ldots, c_{1-1}]$, $[1, c_1, \ldots, c_{1-1}]$ and $[0, 0, 0, c_3, c_4, \ldots, c_{1-1}]$.