Nonadjacent Radix-$\tau$ Expansions of Integers in Euclidean Imaginary Quadratic Number Fields

Ian F. Blake, V. Kumar Murty, and Guangwu Xu

Abstract. In his seminal papers, Koblitz proposed curves for cryptographic use. For fast operations on these curves, these papers also initiated a study of the radix-$\tau$ expansion of integers in the number fields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$. The (window) nonadjacent form of $\tau$-expansion of integers in $\mathbb{Q}(\sqrt{-7})$ was first investigated by Solinas. For integers in $\mathbb{Q}(\sqrt{-3})$, the nonadjacent form and the window nonadjacent form of the $\tau$-expansion were studied. These are used for efficient point multiplications on Koblitz curves. In this paper, we complete the picture by producing the (window) nonadjacent radix-$\tau$ expansions for integers in all Euclidean imaginary quadratic number fields.

Received by the editors December 21, 2005.
AMS subject classification: Primary: 11A63; secondary: 11R04, 11Y16, 11Y40, 14G50.
Keywords: algebraic integer, radix expression, window nonadjacent expansion, algorithm, point multiplication of elliptic curves, cryptography.