OPTIMAL REPRESENTATIONS OF GAUSSIAN AND EISENSTEIN INTEGERS USING DIGIT SETS CLOSED UNDER MULTIPLICATION

EDITA PELANTOVÁ

We discuss an enumeration problem in two number systems, each one given by base $\beta \in \mathbb{C}$ and by set of digits $\mathcal{D} \subset \mathbb{C}$.

- Case 1: $\beta = \imath - 1$ and $\mathcal{D} = \{0, \pm 1, \pm \imath\}$,
- Case 2: $\beta = \omega - 1$ and $\mathcal{D} = \{0, \pm 1, \pm \omega, \pm \omega^2\}$, where $\omega = \exp(2\pi\imath/3)$.

The set $\left\{ \sum\limits_{k=0}^{N-1} d_k \beta^k \,:\, N \in \mathbb{N}\,,\, d_k \in \mathcal{D} \right\}$ equals the ring of Gaussian integers $\mathbb{Z}[\imath]$ in Case 1, and the ring of Eisenstein integers $\mathbb{Z}[\omega]$ in Case 2.
Efficiency of multiplication algorithms in the two systems is guaranteed by three properties:

- Digit set $\mathcal{D}$ is closed under multiplication.
- Addition can be done by a p-local function, multiplication can be performed by on-line algorithms.
- In Case 1, any $x \in \mathbb{Z}[\imath]$ has the w-NAF representation (non-adjacent form) with $w = 3$, and this representation has the minimal Hamming weight among all representations of x. In Case 2, the same is true for any $x \in \mathbb{Z}[\omega]$ with $w = 2$.

We count the number $f(x)$ of optimal representations of $x \in \mathbb{Z}[\beta]$, i.e., representations of x with the minimal Hamming weight. For any fixed $N \in \mathbb{N}$, we determine the maximal and the average value of $f(x)$, where x belongs to $\mathcal{M}_N = \{x \in \mathbb{Z}[\beta] :\ \text{length of } w\text{-NAF representation of } x \text{ is at most } N\}$.