ABSTRACT

RING OF EISENSTEIN INTEGERS: STRUCTURE AND APPLICATIONS

By

ABDUL HADI

22/495359/SPA/00841

We explore the ring of Eisenstein integers as an extension of the ring $\mathbb{Z}$. An Eisenstein prime is an Eisenstein integer that cannot be factored into two non-unit Eisenstein integers. An even Eisenstein integer is a multiple of an Eisenstein prime with the least norm, while all other Eisenstein integers are classified as odd. An Eisenstein integer that is not an integer multiple of another one is said to be primitive. In this work, we establish the algebraic properties of prime, even, odd, primitive Eisenstein integers, the quotient ring, and the set of all unit elements in the quotient ring of Eisenstein integers. Some results are used as algebraic tools in applications in signal constellations and RSA-like cryptosystems.

We propose constructions of signal constellations over quotient rings of Eisenstein integers, equipped with Euclidean and hexagonal distances, generalizing those over Eisenstein integer fields. By set partitioning, we divide a quotient ring of Eisenstein integers into equal-sized subsets. In Eisenstein integer fields of prime size, partitioning is not feasible due to structural limitations. In our setup, we can partition a quotient ring based on additive subgroups, and a set of all unit elements in the quotient ring that forms a cyclic group based on a multiplicative subgroup in such a way that the minimum distances within each subset are larger than or equal to those in the original set. This technique facilitates multilevel coding and enhances the signal constellation's efficiency. Finally, we introduce a novel RSA-like cryptosystem based on the algebraic structure of Eisenstein integers.

INTISARI

RING BILANGAN BULAT EISENSTEIN: STRUKTUR DAN APLIKASI

Oleh

ABDUL HADI

22/495359/SPA/00841

Ring bilangan bulat Eisenstein dikaji sebagai perluasan dari ring $\mathbb{Z}$. Bilangan Eisenstein prima adalah bilangan Eisenstein yang tidak dapat difaktorkan sebagai hasil kali dua bilangan bulat Eisenstein non-unit. Bilangan Eisenstein genap adalah kelipatan dari bilangan Eisenstein prima dengan norma terkecil, sedangkan bilangan lainnya disebut ganjil. Bilangan Eisenstein yang bukan kelipatan bulat dari bilangan Eisenstein lain disebut primitif. Dalam karya ini, sifat-sifat aljabar bilangan Eisenstein prima, genap, ganjil, primitif, ring kuosien, dan himpunan semua elemen unit dalam ring kuosien bilangan bulat Eisenstein dibahas. Kemudian, beberapa hasil digunakan sebagai pendekatan aljabar dalam aplikasi pada konstelasi sinyal dan kriptografi RSA.

Konstruksi konstelasi sinyal atas ring kuosien bilangan bulat Eisenstein yang dilengkapi dengan jarak Euclidean dan jarak heksagonal sebagai generalisasi konstruksi serupa atas lapangan hingga Eisenstein diusulkan. Melalui pembagian himpunan (*set partitioning*), ring kuosien bilangan bulat Eisenstein dibagi menjadi himpunan-himpunan berukuran sama. Berbeda dengan lapangan hingga Eisenstein berukuran prima, yang mana pembagian tidak mungkin dilakukan karena batasan struktural. Kami membagi ring kuosien berdasarkan subgrup penjumlahan, dan himpunan semua elemen unit di ring kuosien yang merupakan grup siklik berdasarkan grup perkalian sedemikian rupa sehingga jarak minimum setiap himpunan bagian lebih besar atau sama dengan di himpunan asli. Teknik ini memfasilitasi pengkodean multilevel dan meningkatkan efisiensi konstelasi sinyal. Terakhir, sistem kriptografi baru yang mirip RSA berdasarkan struktur aljabar ring bilangan bulat Eisenstein dikenalkan.