ABSTRAK

SOLVING DIOPHANTINE EQUATIONS USING MODULAR ARITHMETIC IN RING OF GAUSSIAN INTEGER $\mathbb{Z}[i]$

By

NOVIA LOVIRMA

A Diophantine equation is a polynomial equation over $\mathbb{Z}$ in n variables in which we look for integer solutions. In what follows, we call a *Diophantine equation* an equation of the form $f(x_1, x_2, \ldots, x_2) = 0$, where f is an n-variable function with $n \geq 2$. There are three basic problems arise in concerning a Diopjantine equation :is the equation solvable?, if it is solvable, and is the number of its solutions finite or infinite? It is easier to show that a Diophantine Equations has no solutions than it is to solve an equations with a solution. Elementary methods in solving Diophantine equations, such as decomposition, modular arithmetic, mathematical induction, and Fermat's infinite descent. Althought, some advanced methods for solving Diophantine equations involving *Gaussian integers*, quadratic rings, divisors of certain forms, and quadratic reciprocity.

A Gaussian integer is a complex number whose real part and imaginary part are both integers. The Gaussian integers, with ordinary addition and multiplication of complex numbers, form an integral domain , usually denoted by $\mathbb{Z}[i]$. This domain cannot be turned into an ordered ring, since it contains a square root of -1. Formally, the set of Gaussian integers is $\mathbb{Z}[i] = \{a + bi: a, b \in \mathbb{Z}\}$.

Keyword : *Diophantine equations, ring of Gaussian integer* $\mathbb{Z}[i]$*, prima, divisibility, norm.*