БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра дискретной математики и алгоритмики

Аннотация к дипломной работе

«Свойства теоретико-числовых алгоритмов в факториальных кольцах и их приложения в криптографии»

Кондратёнок Никита Васильевич

Научный руководитель – кандидат физ.-мат. наук, доцент Васьковский М. М.

Минск, 2019

Реферат

Дипломная работа, 66 страниц, 33 источника.

ИДЕАЛ, ФАКТОРИАЛЬНОЕ КОЛЬЦО, ДЕДЕКИНДОВО КОЛЬЦО, ТЕОРЕМА КРОНЕКЕРА-ВАЛЕНА, МЕТОДЫ АВТОМАТИЧЕСКОГО ДОКАЗАТЕЛЬСТВА, RSA-КРИПТОСИСТЕМА

Объектом исследования в данной работе является теорема Кронекера-Валена в числовых полях, методы автоматического доказательства теорем и их приложения в криптографии.

Цель работы состоит в исследовании теоремы Кронекера-Валена в факториальных кольцах. В частности, в нахождении множества колец, в которых теорема верна и разработка метода доказательства неверности теоремы в фиксированном кольце. В построении аналога RSA-криптосистемы в дедекиндовых кольцах и доказательстве основных теорем, связанных с ее криптостойкостью.

Основными методами исследования в работе являются методы теории чисел.

Результатами работы являются специальный класс колец, в котором теорема Кронекера-Валена верна, а так же метод доказательства невыполнимо-сти теоремы Кронекера-Валена. В частности, в работе показано, что теорема Кронекера-Валена не выполняется во всех действительных квадратичных норменно-евклидовых кольцах. В работе разработан аналог RSA-криптосистемы в дедекиндовых кольцах и доказан ряд теорем, связанных с ее безопасностью.

Abstract

Diploma thesis, 66 pages, 33 sources.

IDEAL, UNIQUE FACTORIZATION DOMAIN, DEDEKIND RING, THE KRONECKER-VAHLEN THEOREM, AUTOMATIC PROOF METHODS, RSA-CRYPTOSYSTEM

The object of study in this paper is the Kronecker-Vahlen theorem in numerical fields, methods of automatic proof of theorems and their applications in cryptography.

The aim of the work is to study the Kronecker-Vahlen theorem in unique factorization domains. In particular, in finding the set of rings in which the theorem holds and developing a method to prove that the theorem fails in a fixed ring. Also in constructing an analogue of the RSA cryptosystem in Dedekind rings and the proof of the main theorems related to its cryptographic strength.

The main methods of research in this paper are methods of number theory. The results of the work are a special class of rings in which the Kronecker-

Vahlen theorem holds, as well as a method for proving that the Kronecker-Vahlen theorem fails for fixed ring. In particular, the paper shows that the Kronecker-Vahlen theorem fails in all real quadratic norm-Euclidean rings. An analogue of the RSA-cryptosystem in Dedekind rings is developed and a number of theorems related to its security are proved.