БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра дискретной математики и алгоритмики

Аннотация к магистерской диссертации

«Свойства теоретико-числовых алгоритмов в абстрактных числовых кольцах»

Кондратёнок Никита Васильевич

Научный руководитель – доктор физико-математических наук, доцент
Васьковский М. М.

Минск, 2021

Реферат

Работа, страницы: 63, главы: 2, источники: 36.

RSA-КРИПТОСИСТЕМА, АЛГЕБРАИЧЕСКОЕ ЧИСЛОВОЕ ПОЛЕ, ДЕДЕКИНДОВО КОЛЬЦО, ДЕЛЕНИЕ С ОСТАТКОМ, ИДЕАЛ, КООРДИНАТНОЕ КОЛЬЦО, МЕТОД ПОВТОРНОГО ШИФРОВАНИЯ, МЕТОДЫ АВТОМАТИЧЕСКОГО ДОКАЗАТЕЛЬСТВА, ТЕОРЕМА ВИНЕРА, ТЕОРЕМА КРОНЕКЕРА-ВАЛЕНА, ФАКТОРИАЛЬНОЕ КОЛЬЦО

Объект исследования – теоретико-числовые алгоритмы в абстрактных числовых кольцах. В частности теорема Кронекера-Валена, методы автоматического доказательства теорем, криптографические алгоритмы.

Цель работы – изучение выполнимости теоремы Кронекера-Валена в различных факториальных кольцах. Разработка метода автоматического доказательства выполнимости или невыполнимости теоремы в конкретном кольце. Так же изучение свойств RSA-криптосистемы в дедекиндовых кольцах.

Методы исследования – изучение литературы, методы теории чисел.

Область применения – все сферы науки, в которых исследуемая задача имеет применение.

Результаты работы изложены в двух главах.

Первая глава посвящена изучению аналога RSA-криптосистемы в дедекиндовых кольцах. Изучена применимость метода повторного шифрования, доказан аналог теоремы Винера и других теорем, связанных с ее безопасностью. Показано, что задача факторизации идеала полиномиально сводится к задаче факторизации в целых числах.

Вторая глава посвящена теореме Кронекера-Валена. Выделен класс факториальных колец, в которых эта теорема верна. Разработан алгоритм проверки достаточного условия принадлежности факториального кольца этому классу. Используя эти алгоритмы, приведены примеры колец, для которых теорема Кронекера-Валена верна. Разработан метод доказательства невыполнимости теоремы Кронекера-Валена. Доказано, что теорема Кронекера-Валена не выполняется в действительных квадратичных норменно-евклидовых кольцах.

Abstract

Paper, pages: 63, chapters: 2, sources: 36.

RSA-CRYPTOSYSTEM, ALGEBRAIC NUMBER FIELD, DEDEKIND RING, DIVISION WITH REMAINDER, IDEAL, COORDINATE RING, RE-ENCRYPTION METHOD, AUTOMATIC PROOF METHODS, WIENER THEOREM, KRONECKER-VALEN THEOREM, FACTORIAL RING

Object of research – number-theoretic algorithms in abstract number rings. In particular, the Kronecker-Walen theorem, methods of automatic theorem proving, cryptographic algorithms.

The purpose of this work is to study the satisfiability of the Kronecker-Wahlen theorem in various factorial rings. Development of a method for automatically proving the feasibility or non-feasibility of a theorem in a specific ring. Also, the study of the properties of the RSA-cryptosystem in Dedekind rings.

Research methods – study of literature, methods of number theory.

Application area – areas of science in which the problem has applications.

The results of the work are presented in two chapters.

The first chapter is devoted to the study of an analogue of the RSA cryptosystem in Dedekind rings. The applicability of the re-encryption method is studied, an analogue of Wiener's theorem and other theorems related to its security is proved. It is shown that the problem of factorizing an ideal is polynomially reduced to the problem of factoring in integers.

The second chapter is devoted to the Kronecker-Walen theorem. A class of factorial rings is distinguished in which this theorem is true. An algorithm for checking a sufficient condition for a factorial ring to belong to this class is developed. Using these algorithms, examples of rings are given for which the Kronecker-Walen theorem is true. A method for proving the impossibility of the Kronecker-Walen theorem is developed. It is proved that the Kronecker-Walen theorem does not hold in real quadratic norm-Euclidean rings.