ОТЗЫВ

на автореферат диссертации **Кондратенка Никиты Васильевича «Свойства теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах»**, представленной на соискание ученой степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел

В диссертации доказываются новые критерии простоты идеалов в дедекиндовых кольцах. Эти критерии являются аналогами критериев Эйлера и Миллера и позволяют строить эффективные тесты на простоту в дедекиндовых кольцах.

В диссертации разработаны новые подходы к исследованию экстремальных свойств цепочек делений в факториальных кольцах.

Целью диссертации является доказательство новых критериев простоты идеалов в дедекиндовых кольцах и исследование свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах.

В работе:

1. Доказаны критерии простоты идеалов в дедекиндовых кольцах, аналогичные критериям Эйлера и Миллера в кольце целых чисел. Показано, что полученные критерии можно использовать для построения эффективных вероятностных алгоритмов проверки идеала на простоту. Получены достаточные условия для дедекиндового кольца для того, чтобы этот алгоритм можно было модифицировать и сделать детерминированным. Получены оценки вычислительной сложности алгоритмов.

2. Доказаны теоремы об экстремальных свойствах алгоритма Евклида в факториальных кольцах. Получен класс колец, в которых верна теорема Кронекера-Валена. Разработан алгоритм, позволяющий проверить принадлежность кольца этому классу колец. Построен метод автоматического доказательства невыполнимости теоремы Кронекера-Валена в числовых кольцах. Доказано, что теорема Кронекера-Валена не выполняется во всех действительных квадратичных норменно-евклидовых кольцах.

3. Доказан аналог теоремы Ламе о длине цепочки делений с выбором минимального по норме остатка в факториальных кольцах. Доказаны теоремы накладывающие необходимые условия на параметры аналога криптосистемы RSA в дедекиндовых кольцах для обеспечения устойчивости к взлому. В частности, теорема Винера о малой секретной экспоненте и теорема Кранакиса.

С технической точки зрения нахождение больших простых чисел является очень сложной задачей требующей больших вычислительных ресурсов. Способы и методы сокращения вычислений простых чисел представленные в диссертации являются важными и актуальными. Они могут применяться в широкой сфере жизнедеятельности человека от обеспечения сохранности личных данных, безопасности платежей и переводов до шифрования сообщений государственного значения.

В качестве замечания отмечу следующее: в автореферате не представлена сравнительная оценка эффективности предлагаемого алгоритма нахождения простых чисел по отношению к известным.

Указанные замечания не снижают общей ценности диссертационной работы и положений выносимых на защиту.

В целом работа, судя по автореферату, представляет законченное исследование и удовлетворяет требованиям ВАК, а ее автор, Кондратенок Н.В., заслуживает присуждения ему степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Профессор кафедры автоматики,
радиолокации и приёмопередающих устройств
учреждения образования «Военная академия
Республики Беларусь»

к.т.н., доцент А.С. Солонар

24.01.2023

Я, Солонар Андрей Сергеевич, даю согласие на обработку моих персональных данных, связанную с защитой диссертации и оформлением аттестационного дела Кондратенка Никиты Васильевича.

А.С. Солонар

Подпись Солонара Андрея Сергеевича заверяю.

Начальник отдела кадров
учреждения образования
«Военная академия
Республики Беларусь»
полковник В.В.Щербин

24.01.2023