ЗАКЛЮЧЕНИЕ

совета по защите диссертаций Д 01.02.01
при государственном научном учреждении «Институт математики НАН Беларуси»
по диссертации **Кондратёнка Никиты Васильевича**
«Свойства теоретико-числовых и криптографических алгоритмов
в дедекиндовых кольцах»,
представленной на соискание учёной степени кандидата физико-математических наук
по специальности 01.01.06 – математическая логика, алгебра и теория чисел

1. Специальности и отрасль науки, по которой присуждается искомая ученая степень.

В соответствии с перечнем специальностей и отраслей науки, утвержденным ВАК Республики Беларусь, диссертационная работа, представленная на соискание учёной степени кандидата физико-математических наук, соответствует специальности 01.01.06 – математическая логика, алгебра и теория чисел (физико-математические науки).

2. Научный вклад соискателя в решение научной задачи с оценкой его значимости.

Диссертационная работа Н.В. Кондратёнка содержит новые научные результаты, относящиеся к алгоритмической теории чисел. Доказаны новые критерии простоты идеалов в дедекиндовых кольцах, обобщающие известные критерии Миллера и Эйлера, что позволило построить новые эффективные алгоритмы тестирования идеалов на простоту; доказаны новые теоремы о длине цепочек делений в факториальных кольцах, на основе которых доказаны аналоги теорем Кронекера-Валена и Ламе для некоторого класса факториальных колец; доказано, что теорема Кронекера-Валена не выполняется в кольце целых элементов действительного квадратичного числового поля, исследованы свойства аналога криптосистемы RSA в дедекиндовых кольцах и найдены условия криптостойкости этой криптосистемы. Приведенные в диссертации результаты в совокупности вносят значительный вклад в развитие алгоритмической теории чисел и ее приложениях к криптографии.

3. Конкретные научные результаты, за которые соискателю может быть присуждена ученая степень, их новизна и практическая значимость.

Совет по защите диссертаций Д 01.02.01 в соответствии с Положением о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь постановляет присудить Кондратёнку Никите Васильевичу ученую степень кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел – за новые научно-обоснованные результаты в области алгоритмической теории чисел, включающие:

критерии простоты идеалов в дедекиндовых кольцах с конечной нормой;

теоремы о длине цепочек делений в факториальных кольцах;

необходимые условия криптографической стойкости криптосистемы RSA в дедекиндовых кольцах.

4. Рекомендации по использованию результатов исследования.

Полученные в диссертации результаты найдут применение в исследованиях свойств теоретико-числовых и криптографических алгоритмов в дедекиндовых кольцах или кольцах более общего вида, а также будут полезны при чтении спецкурсов для студентов математических специальностей, в том числе при подготовке курсовых и дипломных работ, магистерских диссертаций.

Председатель совета
по защите диссертаций Д 01.02.01
академик В.И. Янчевский

Ученый секретарь совета
по защите диссертаций Д 01.02.01
кандидат физико-математических наук Т.С. Бусел