

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра математической кибернетики**

ВОЛКОВА
Анна Дмитриевна

**АППАРАТНЫЕ АЛГОРИТМЫ ВЫЧИСЛЕНИЙ
В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ**

Дипломная работа

Научный руководитель:
кандидат физико-
математических наук,
старший преподаватель
Ю. Г. Таразевич

Допущен к защите

«__» _____ 2022 г.

Заведующий кафедрой математической кибернетики,
доктор физико-математических наук, профессор А. Л. Гладков

Минск, 2022

РЕФЕРАТ

Дипломная работа: 54 с., 10 рис., 2 табл., 13 источников.

Ключевые слова: система остаточных классов, аппаратные алгоритмы, модульные операции, немодульные операции.

Объект исследования: аппаратные алгоритмы вычислений в системе остаточных классов

Цель исследования: рассмотреть различные варианты аппаратных вычислений для каждой арифметической операции, выявить и привести сравнительные характеристики эффективности вычислений для каждой из рассматриваемых операций.

Методы исследования: анализ технической литературы, исследование алгоритмов в системе остаточных классов с различными значениями и сравнение полученных результатов.

В ходе выполнения работы рассмотрена система остаточных классов, а также были рассмотрены различные алгоритмы модульных и немодульных операций в системе остаточных классов. Для каждой арифметической операции были рассмотрены различные варианты аппаратных вычислений и приведены разнообразные примеры выполнения этих алгоритмов. Результатом выполнения работы является сравнительная характеристика для каждой из рассматриваемых операций.

Область применения: криптография, цифровая обработка сигналов, высоконадежные облачные хранилища, блокчейн-технологии, вычисления многократной точности, нейронные сети.

ABSTRACT

Degree paper: 54 pp., 10 pics, 2 tables, 13 sources.

Keywords: residual number system, hardware algorithms, modular operations, non-modular operations.

Object of research: hardware computing algorithms in the system of residual classes

Purpose of research: to consider various options for hardware calculations for each arithmetic operation, to identify and present comparative characteristics of the computational efficiency for each of the operations under consideration.

Research methods: analysis of technical literature, study of algorithms in the system of residual classes with different values and comparison of the results obtained.

In the course of the work, the system of residual classes was considered, and various algorithms for modular and non-modular operations in the system of residual classes were considered. For each arithmetic operation, various options for hardware calculations were considered and various examples of the implementation of these algorithms were given. The result of the work is a comparative characteristic for each of the considered operations.

Area of possible practical application: cryptography, digital signal processing, highly reliable cloud storage, blockchain technologies, multiple precision calculations, neural networks.

РЭФЕРАТ

Дыпломная праца: 54 с., 10 мал., 2 табл., 13 крыніц.

Ключавыя словы: сістэма рэшткавых класаў, апаратныя алгарытмы, модульныя аперацыі, немодульныя аперацыі.

Аб'ект даследавання: апаратныя алгарытмы вылічэнняў у сістэме рэшткавых класаў

Мэта даследавання: разгледзець розныя варыянты апаратных вылічэнняў для кожнай арыфметычнай аперацыі, выявіць і прывесці параўнальныя характарыстыкі эфектыўнасці вылічэнняў для кожнай з разгляданых аперацый.

Метады даследавання: аналіз тэхнічнай літаратуры, даследаванне алгарытмаў у сістэме рэшткавых класаў з рознымі значэннямі і параўнанне атрыманых вынікаў.

У ходзе выканання работы разгледжана сістэма рэшткавых класаў, а таксама былі разгледжаны розныя алгарытмы модульных і немодульных аперацый у сістэме рэшткавых класаў. Для кожнай арыфметычнай аперацыі былі разгледжаны розныя варыянты апаратных вылічэнняў і прыведзены разнастайныя прыклады выканання гэтых алгарытмаў. Вынікам выканання працы з'яўляецца параўнальная характарыстыка для кожнай з разгляданых аперацый.

Вобласць магчымага практычнага прымянення: крыптаграфія, лічбавая апрацоўка сігналаў, высоканадзейныя хмарныя сховішчы, блокчэйн-тэхналогіі, вылічэнні шматразовай дакладнасці, нейронавыя сеткі.