

Модель с подстройкой параметров для модулярных вычислений в больших компьютерных диапазонах

С.А. Инютин, В.О. Иванов

Московский авиационный институт (национальный исследовательский университет)

Современные вычислительные задачи в области теории чисел часто требуют обработки числовых значений, значительно превышающих возможности стандартных компьютерных архитектур. Особую сложность представляют операции с числами специального вида и тестирование на простоту, где традиционные методы сталкиваются с фундаментальными ограничениями. Модулярная арифметика предлагает принципиально иной подход к решению этих задач, обеспечивая не только работу с числами произвольной величины, но и естественный параллелизм вычислений [1].

Предлагаемая модель основана на тщательном подборе параметров модулярной системы, включая выбор оптимальных оснований. Ключевым аспектом является минимизация бивалентного эффекта, который возникает при отображении модулярных вычетов в двоичных регистрах. Для этого предлагается использовать пары простых чисел, симметрично расположенных относительно степеней двойки (2^{31} , 2^{32} , 2^{64}). Такой подход позволяет максимально эффективно использовать стандартные 32- и 64-разрядные регистры современных процессоров [2, 3].

Для практической реализации модели были разработаны три специализированных алгоритма на языке Python. Особое внимание уделено оптимизации производительности: применение библиотеки Numba с компилятором LLVM позволило ускорить вычисления в 40–50 раз. Для работы с особо большими числами (2^{64}) была дополнительно использована высокопроизводительная программа primesieve, написанная на C++. Эти решения обеспечили эффективный поиск симметричных простых чисел даже в экстремально больших диапазонах. Алгоритмы дают одинаковый результат при их выполнении, что подтверждает их взаимную правильность.

Разработанная модель имеет значительный потенциал для применения в различных областях, включая криптографию, обработку сигналов и вычислительную теорию чисел. Особую ценность представляют возможности параллельной обработки данных и устойчивость к ошибкам, что делает модулярные вычисления перспективным направлением для создания высокопроизводительных вычислительных систем. Дальнейшие исследования могут быть направлены на адаптацию модели для работы с еще большими числовыми диапазонами и специализированными аппаратными архитектурами.

Литература

1. Инютин С.А. Модулярная алгоритмика многоразрядных вычислений. М.: Изд-во МАИ, 2020. 160 с.
2. Инютин С.А. Модулярные процессоры – оценки, история борьбы и победы над бивалентным дефектом // Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы. SoRuCom-2017: сб. тр. IV Междунар. конф., Зеленоград, 3–5 октября 2017 / под ред. д.ф.-м.н. А.Н. Томилина. М.: РЭУ им. Г.В. Плеханова, 2017. С. 72–77.
3. Эрдниева Н.С. Использование специальных модулей системы остаточных классов для избыточного представления // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. 2013. № 2. С. 75–84.