

Терещенко Андрій Миколайович
кандидат фізико-математичних наук

Ефективні алгоритми реалізації багаторозрядного множення на основі перетворення Мерсенна

Операція багаторозрядного множення використовується для реалізації криптографічних алгоритмів та є однією з операцій, які впливають на швидкість асиметричних криптографічних операцій таких, як шифрування, дешифрування, верифікація електронного цифрового підпису. Використання швидких методів дозволяє виконувати операції з меншою складністю або на пристроях з меншим набором команд, які не мають операції з плаваючою комою. Такими методами є методи, які використовують перетворення Мерсенна.

Розглядається оптимізація реалізації багаторозрядного множення на основі дискретного ортогонального перетворення Мерсенна. Надані основні переваги алгоритму реалізації багаторозрядного множення на основі перетворення Мерсенна. Коротко розглянуто алгоритм багаторозрядного множення на основі перетворення Мерсенна з найменшим примітивним коренем, який дорівнює 2, та наведені деякі властивості алгоритмів на основі чисел Мерсенна. У вигляді формули наведена межа максимально можливого значення множника, яка залежить від довжини p перетворення Мерсенна. Наведено швидкий алгоритм обчислення залишку числа за модулем числа Мерсенна, який значно зменшує складність алгоритму множення. Наведена формула обчислення оберненого числа, необхідного для обчислення оберненого перетворення Мерсенна великої довжини.

Надано обмеження оптимізації алгоритмів на основі теоретико-числових перетворень (ТЧП), які пов'язані з тим, що довжина такого перетворення дорівнює простому числу, що ускладнює розбиття ТЧП на менші матриці з метою прискорення обчислень. Надано аналіз деяких методів оптимізації ТЧП, які дозволяють представити матрицю степенів двійки перетворення Мерсенна у вигляді циркулярної матриці, оптимізація обчислення якої можлива з використанням швидких методів обчислення коротких циклічних матриць. Звертається увагу на те, що навіть використання невеликої кількості операцій множення для заміни операцій додавання та побітового зсуву (які є основними операціями для обчислення прямого та оберненого перетворення Мерсенна) «поглинає» ефект прискорення.

Наведено ефективний алгоритм реалізації багаторозрядного множення на основі перетворення Мерсенна за рахунок використання циклічної згортки, елементами якої є багаторозрядні числа. Даний метод дозволяє обчислення дискретного перетворення Мерсенна замінити обчисленням дискретних перетворень Мерсенна меншого розміру, що пришвидшує загальний час приблизно на 18 відсотків.

На основі властивостей чисел Мерсенна показано, що піднесення до квадрату числа довжиною $2N$ слів за модулем числа Мерсенна, може бути представлена у вигляді двох множень чисел довжиною N слів, що на одне множення менше ніж множення без модуля, яке потребує щонайменше три множення. Даний метод прискорює багаторозрядну операцію піднесення до квадрату за модулем на 33 відсотки. Аналогічно показано, що піднесення до квадрату числа довжиною $3N$ слів за модулем числа Мерсенна, може бути представлено у вигляді трьох піднесень до квадрату та двох множень чисел довжиною N слів. Піднесення до квадрату числа довжиною $4N$ слів за модулем числа Мерсенна, може бути представлено у вигляді семи піднесень до квадрату та одного множення чисел довжиною N слів.

Показано, що в алгоритмі, який використовує велику кількість операцій додавання, «вузьким місцем» швидкодії є операція перевірки та врахування знаку переносу. Використання швидкого алгоритму перевірки знаку переносу та 64-бітних операцій додавання дозволяє зменшити загальний час виконання багаторозрядної операції у два рази.

Для перевірки коректності алгоритм було реалізовано на двох різних мовах програмування C# (з використанням бібліотеки програм BigInteger) та C++.

Результати доповіді можуть бути використані для реалізації швидких алгоритмів багаторозрядної арифметики та для реалізації у мікросхемному виконанні та на ПЛІСax.