Пошук канонічного розкладу великого числа, використовуючи відомі методи факторизації

1 Мета

Практичне ознайомлення з різними методами факторизації чисел, реалізація цих методів і їх порівняння. Виділення переваг, недоліків та особливостей застосування алгоритмів факторизації. Застосування комбінації алгоритмів факторизації для пошуку канонічного розкладу заданого числа.

2 Постановка задачі

Створити та реалізувати алгоритм для пошуку канонічного розкладу числа.

3 Хід роботи

Програма використовує кілька алгоритмів для знаходження канонічного розкладу числа. Спочатку перевіряється, чи є число простим за допомогою тесту Соловея-Штрассена, який використовує символ Якобі для визначення простоти числа з певною ймовірністю. Якщо число не є простим, використовується метод пробних ділень для знаходження дільників, які не перевищують 47. Якщо дільник не знайдено, застосовується метод Полларда для пошуку дільників шляхом випадкового перебору. У випадку, коли всі інші методи не знаходять дільник, застосовується метод Брілгарта-Моррісона.

У нас виникди труднощі з реалізацією алгоритму Брілгарта-Моррісона, який для великих чисел працює дуже довго.

4 Приклад роботи програми

Запустивши програму для числа 3009182572, маємо такий вивід:
Processing number: 3009182572
Divisor found: 2, using method: Trial Division, at time: Thu Mar 21 20:40:01 2024
Divisor found: 2, using method: Trial Division, at time: Thu Mar 21 20:40:01 2024
Divisor found: 11, using method: Trial Division, at time: Thu Mar 21 20:40:01 2024
Divisor found: 2063, using method: Pollard's Rho, at time: Thu Mar 21 20:40:01 2024
Divisor found: 33151, using method: Solovay-Strassen (primality test), at time: Thu Mar 21 20:40:01 2024
Algorithm execution time: 0.00661767s
Canonical expansion: 2 2 11 2063 33151

5 Замір часу роботу мутоду Полларда

Запустивши функцію для вхідних значень різної довжини, отримали, що середній час 0.163927 ms.

6 Висновок

У цій роботі було розроблено програму для знаходження канонічного розкладу числа, використовуючи різноманітні методи факторизації, дана програма може бути вдосконалена, особливу увагу потрібно звернути на пошук гладки чисел для методу Брілгарта-Моррісона.