

Міністерство освіти і науки України
Національний технічний університет України "Київський політехнічний інститут
імені Ігоря Сікорського"
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

ЗВІТ

Лабораторна робота №3.1

з дисципліни
«Інтелектуальні вбудовані системи»

на тему
«Реалізація задачі розкладання числа на прості множники
(факторизація числа)»

Виконав:
Василиненко Д.Д.
Студент групи ІП-84
Перевірив:
Регіда Павло Геннадійович

Київ 2021

Завдання

Розробити програма для факторизації заданого числа методом Ферма.
Реалізувати користувацький інтерфейс з можливістю вводу даних

Основні теоретичні відомості

Факторизації лежить в основі стійкості деяких криптоалгоритмів, еліптичних кривих, алгебраїчній теорії чисел та кванових обчислень, саме тому дана задача дуже гостро досліджується, й шукаються шляхи її оптимізації. На вхід задачі подається число $n \in \mathbb{N}$, яке необхідно факторизувати. Перед виконанням алгоритму слід переконатись в тому, що число не просте. Далі алгоритм шукає перший простий дільник, після чого можна запустити алгоритм заново, для повторної факторизації. В залежності від складності алгоритми факторизації можна розбити на дві групи: Експоненціальні алгоритми (складність залежить експоненційно від довжини вхідного параметру); Субекспоненціальні алгоритми. Існування алгоритму з поліноміальною складністю – одна з найважливіших проблем в сучасній теорії чисел. Проте, факторизація з даною складністю можлива на квантовому комп'ютері за допомогою алгоритма Шора. Метод факторизації Ферма. Ідея алгоритму заключається в пошуку таких чисел A і B , щоб факторизоване число n мало вигляд: $n = A^2 - B^2$. Даний метод гарний тим, що реалізується без використання операцій ділення.

Вихідний код:

fermatFactor.ts

```
export const fermaFactor = (n: number): number[] => {  
  if (n <= 0) {  
    return [n];  
  }  
  
  if (!(n % 2)) {  
    return [n / 2, 2];  
  }  
  
  let a = Math.ceil(Math.sqrt(n));  
  
  if (a * a === n) {  
    return [a, a];  
  }  
  
  let b = 0;  
  while (1) {  
    const c = a * a - n;  
    b = Math.floor(Math.sqrt(c));  
  
    if (b * b === c) break;  
    else a += 1;  
  }  
  
  return [a - b, a + b];  
};
```

Результати роботи програми

2468629642542|

1234314821271 * 2

COMPUTE



¹q ²w ³e ⁴r ⁵t ⁶y ⁷u ⁸i ⁹o ⁰p

a s d f g h j k l

↑ z x c v b n m ⌫

?123



QWERTY

.



2468629642545

$1427745 * 1729041$

COMPUTE



q¹ w² e³ r⁴ t⁵ y⁶ u⁷ i⁸ o⁹ p⁰

a s d f g h j k l

↑ z x c v b n m ⌫

?123



QWERTY

.



Висновки

Під час виконання даної лабораторної роботи ми ознайомилися з принципами розкладання числа на прості множники з використанням різних алгоритмів факторизації. Програмно було реалізовано метод факторизації Ферма. Для вводу початкових даних було створено користувацький інтерфейс.