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

3BIT

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

Завдання

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

Основні теоретичні відомості

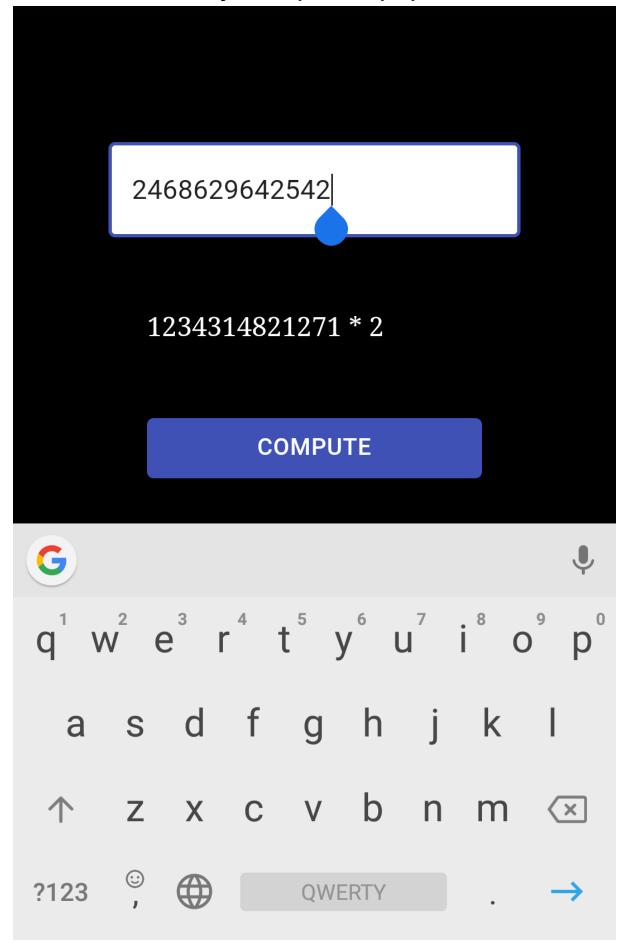
Факторизації лежить в основі стійкості деяких криптоалгоритмів, еліптичних кривих, алгебраїчній теорії чисел та кванових обчислень, саме тому дана задача дуже гостро досліджується, й шукаються шляхи її оптимізації. На вхід задачі подається число п € №, яке необхідно факторизувати. Перед виконанням алгоритму 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 А і В, 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





1427745 * 1729041

COMPUTE





 $q^1 \ w^2 \ e^3 \ r^4 \ t^5 \ y^6 \ u^7 \ i^8 \ o^9 \ p^0$

asdfghjkl

↑ 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.