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

Лабораторна робота №3.1

з дисципліни
«Інтелектуальні вбудовані системи»

на тему
«Неалізація задачі розкладання числа на прості

множники (факторизація числа)»

Виконала:

студентка

групи ІП-83

Гомілко Діана Володимирівна

Перевірив:

Регіда Павло Геннадійович

Київ 2021

Основні теоретичні відомості, необхідні для виконання лабораторної роботи

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 Є 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.

Умови завдання для варіанту

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

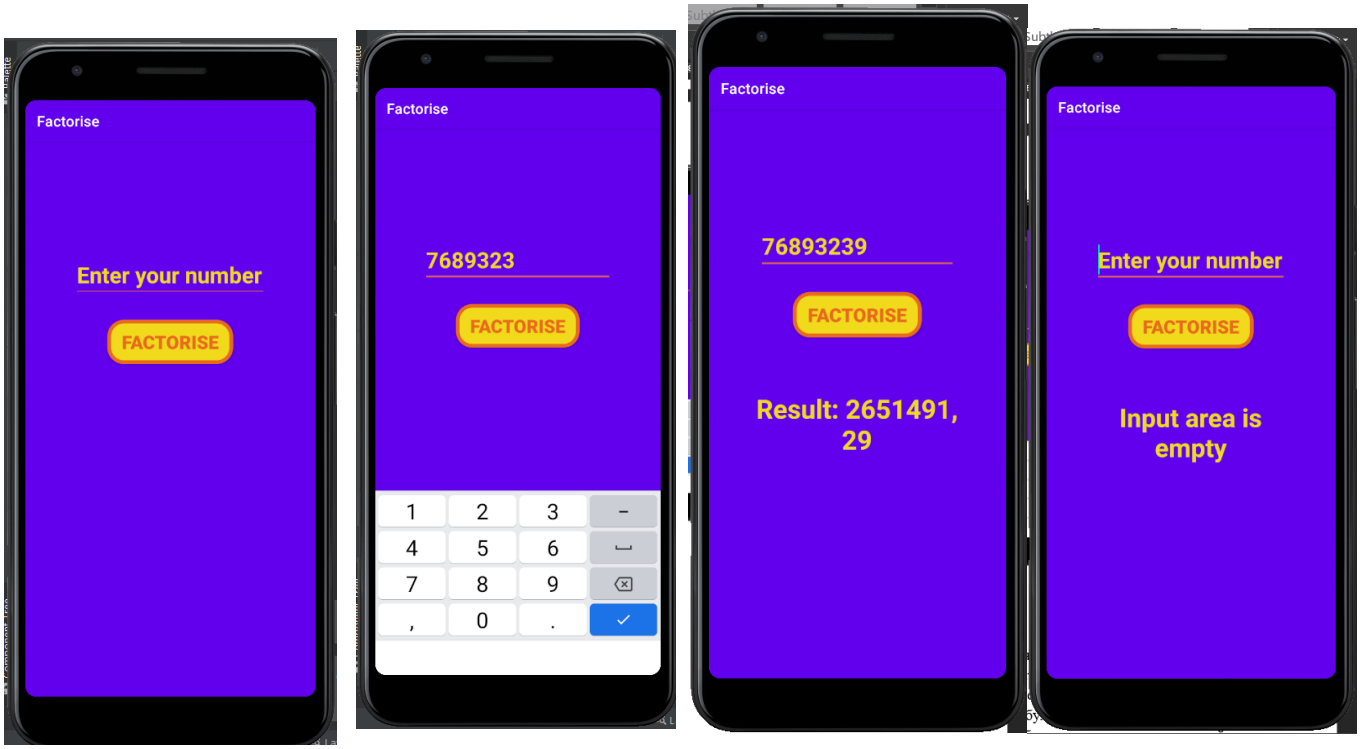
Лістинг програми із заданими умовами завдання

MainActivity.kt

```
package com.example.factorise

import androidx.appcompat.app.AppCompatActivity
import android.os.Bundle
import android.widget.Button
import android.widget.EditText
import android.widget.TextView
import java.lang.Math.ceil
import java.lang.Math.sqrt
import kotlin.math.pow
```

```
class MainActivity : AppCompatActivity() {
    private lateinit var input: EditText
    private lateinit var button: Button
    private lateinit var result: TextView

    override fun onCreate(savedInstanceState: Bundle?) {
        super.onCreate(savedInstanceState)
        setContentView(R.layout.activity_main)

        input = findViewById(R.id.editTextNumber)
        button = findViewById(R.id.factoriseBtn)
        result = findViewById(R.id.textView)

        button.setOnClickListener { handleBtnClick() }
    }

    private fun handleBtnClick() {
        var output = ""
        val text = input.text.toString()
        output = if (text.isEmpty()) "Input area is empty"
        else {
            val n = text.toInt()
            val res = fermatFactorise(n)
            if (res !== null) "Result: ${res.first}, ${res.second}" else "Invalid input
data"
        }
        result.text = output
    }

    private fun fermatFactorise(n: Int): Pair<Int, Int>? {
        if (n <= 0) return null
        if (n % 2 == 0) return Pair(2, n / 2)

        var x = kotlin.math.ceil(kotlin.math.sqrt(n.toDouble()))
        var y = x.pow(2) - n

        while (kotlin.math.sqrt(y) != kotlin.math.ceil(kotlin.math.sqrt(y))) {
            x++
            y = x.pow(2) - n
        }

        val ySqrt = kotlin.math.sqrt(y)
        return Pair((x + ySqrt).toInt(), (x - ySqrt).toInt())
    }
}
```

Результати виконання кожної програми



Висновки щодо виконання лабораторної роботи

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.