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

Виконала:

студентка групи ІП-84

Шахова Поліна Миколаївна
номер залікової книжки: 8424

Перевірив:

ас. Регіда П. Г.

Київ 2020

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 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.

Рис1. Алгоритми факторизації

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, а лише з операціями додавання й віднімання.

Приклад алгоритму:

Початкова установка: $x = [\sqrt{n}]$ – найменше число, при якому різниця x^2-n невід'ємна

Для кожного значення k Є ℕ, починаючи з k = 1, обчислюємо $(\lceil\sqrt{n}\rceil + k)^2 - n$ і перевіряємо чи не є це число точним квадратом.

- Якщо не є, то k++ і переходимо на наступну ітерацію.
- Якщо є точним квадратом, тобто $x^2 - n = (\lceil\sqrt{n}\rceil + k)^2 - n = y^2$, то ми отримуємо розкладання: $n = x^2 - y^2 = (x + y)(x - y) = A * B$, в яких

$$x = (\lceil\sqrt{n}\rceil + k)$$

Якщо воно є тривіальним і єдиним, то n - просте

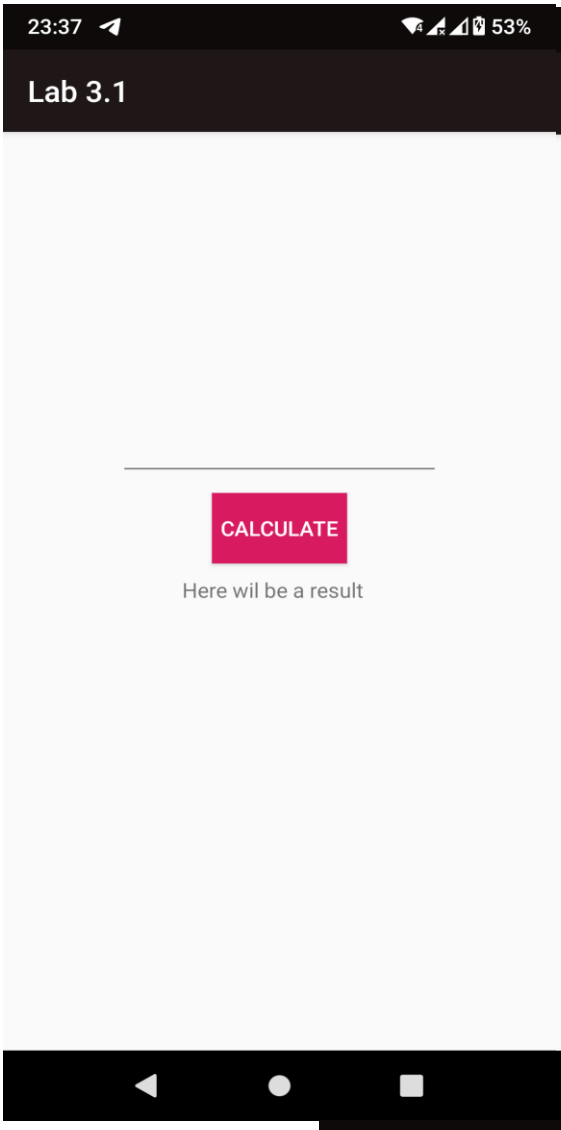
Завдання за варіантом:
Варіант 24

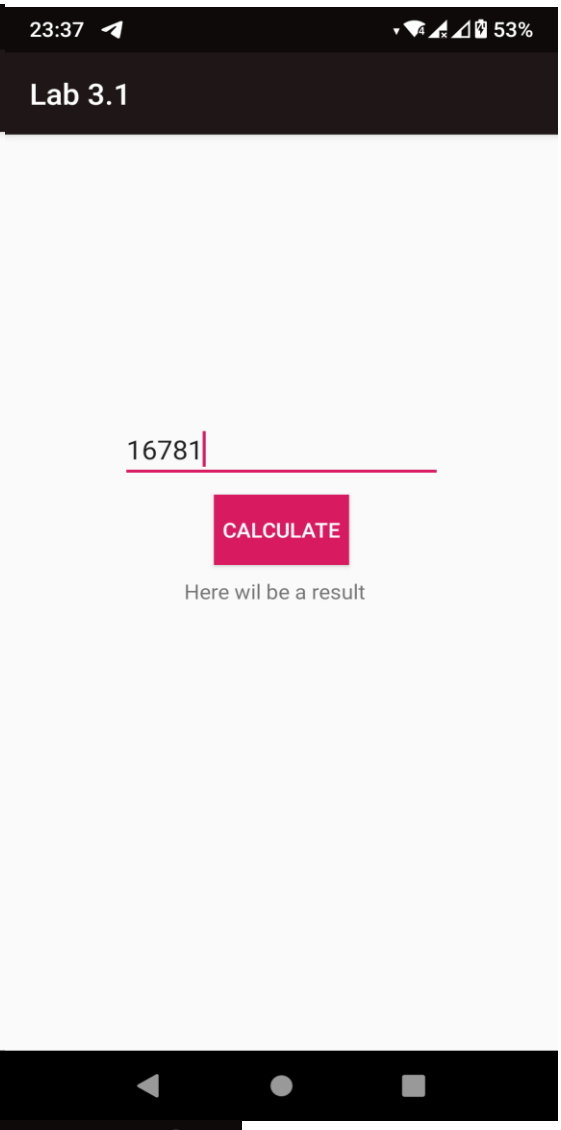
Лістинг програми:

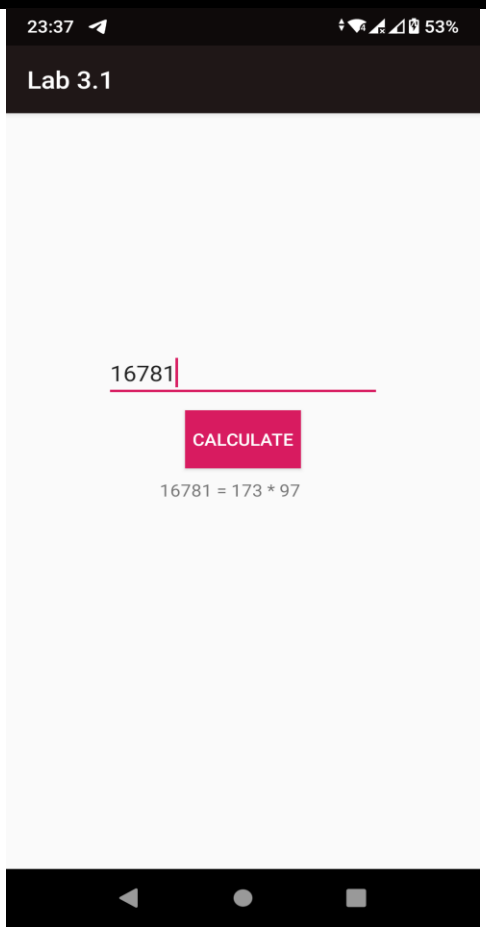
```
package com.example.lab31

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.sqrt
import kotlin.math.*

class MainActivity : AppCompatActivity() {

//    public final var resultTextView : TextView
    private fun isSquare(n: Double) :Boolean{
    var result = (n === ceil(sqrt(n)).pow(2))
    return result
}

    private fun ferma_factorisation(n: Double) :String{
        var a = ceil(sqrt(n))

        while (!isSquare(a.pow(2) - n)){
            a += 1
        }
        var b = sqrt(a.pow(2) - n)
        var result =  "${n.toInt()} = ${(a + b).toInt()} * ${(a -
b).toInt()}"

        return result
    }

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

        var result: TextView = findViewById(R.id.show_result)
        var inputData: EditText = findViewById(R.id.input_data)

        var buttonCalculate: Button = findViewById(R.id.button_calculate)
        buttonCalculate.setOnClickListener {
            if (inputData.text.isEmpty()){
                result.text = "There was no number entered!"
            } else {
                var test:Double = inputData.text.toString().toDouble()
                result.text = ferma_factorisation(test)
            }
        }
    }
```

```
}
```

Приклад роботи програми:


23:37
53%
Lab 3.1
CALCULATE
Here wil be a result


23:37
53%
Lab 3.1
16781
CALCULATE
Here wil be a result


23:37
53%
Lab 3.1
16781
CALCULATE
16781 = 173 * 97

Висновки:

Під час виконання лабораторної роботи я дослідила основні принципи розкладання числа на прості множники з використанням різних алгоритмів факторизації.

Я розробила програму для факторизації заданого числа методом Ферма, реалізовала користувацький інтерфейс з можливістю вводу даних за допомогою Android.