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)»

|  |  |  |
| --- | --- | --- |
|  |  |  |

Виконав: Перевірив:

студент групи ІП-83 викладач  
Фібрук Руслан Сергійович Регіда Павло Геннадійович  
номер залікової книжки: 8320

Київ 2021

**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.

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, а лише з операціями додавання й віднімання. Приклад алгоритму: Початкова установка: x = [√𝑛] – найменше число, при якому різниця x 2 -n невід’ємна. Для кожного значення k Є ℕ, починаючи з k = 1, обчислюємо (⌈√𝑛⌉ + 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 = (⌈√𝑛⌉ + 𝑘) 2 − 𝑛 = 𝑦 2 , то ми отримуємо розкладання: 𝑛 = 𝑥 2 − 𝑦 2 = (𝑥 + 𝑦)(𝑥 − 𝑦) = 𝐴 ∗ 𝐵, в яких 𝑥 = (⌈√𝑛⌉ + 𝑘) Якщо воно є тривіальним і єдиним, то n - просте

**Завдання на лабораторну роботу**

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

**Лістинг програми**

package ua.kpi.comsys.ip8313.lab31  
  
import android.content.Context  
import androidx.appcompat.app.AppCompatActivity  
import android.os.Bundle  
import android.view.inputmethod.InputMethodManager  
import android.widget.Button  
import android.widget.EditText  
import android.widget.Toast  
import kotlin.math.abs  
import kotlin.math.sqrt  
  
class MainActivity : AppCompatActivity() {  
 private fun fermatFactorization(n: Int): Pair<Int, Int> {  
 if (n % 2 == 0) return Pair(2, n / 2)  
 var x = *abs*(*sqrt*(n.toDouble())).toInt()  
 if (x \* x == n) return Pair(x, x)  
 while (true) {  
 val tmp = x \* x - n  
 val y = *sqrt*(tmp.toDouble()).toInt()  
 if (y \* y == tmp) return Pair(x - y, x + y)  
 x++  
 }  
 }  
  
 private fun hideKeyboard() {  
 val imm = this.getSystemService(Context.*INPUT\_METHOD\_SERVICE*) as InputMethodManager  
 imm.hideSoftInputFromWindow(*currentFocus*!!.*windowToken*, 0)  
 }  
  
 override fun onCreate(savedInstanceState: Bundle?) {  
 super.onCreate(savedInstanceState)  
 setContentView(R.layout.*activity\_main*)  
 val inputView = findViewById<EditText>(R.id.*arg\_input*)  
 val submitButton = findViewById<Button>(R.id.*factorize\_button*)  
  
 submitButton.setOnClickListener **{** val input = inputView.*text*.toString()  
 val arg = input.*toIntOrNull*()  
 if (arg == null) {  
 Toast.makeText(this, "Input should be a number!", Toast.*LENGTH\_LONG*).show()  
 }  
 else {  
 val (a, b) = fermatFactorization(arg)  
 hideKeyboard()  
 Toast.makeText(this, "$input = $a \* $b", Toast.*LENGTH\_LONG*).show()  
 inputView.*text*.clear()  
 }  
 **}** }  
}

**Результати роботи програми**

  

**Висновки**

При виконанні цієї лабораторної роботи ми реалізували алгоритм факторизації числа за методом Ферма та створили користувацький інтерфейс для введення аргументу та відображення результату.