Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра обчислювальної техніки

Системи реального часу

Лабораторна робота №3.1

РЕАЛІЗАЦІЯ ЗАДАЧІ РОЗКЛАДАННЯ ЧИСЛА НА ПРОСТІ

МНОЖНИКИ (ФАКТОРИЗАЦІЯ ЧИСЛА)

Виконав:

студент групи ІО-72

Воронін О.Г.

Номер залікової книжки № 7203

Номер у списку - 2

Перевірив Регіда П.Г.

Київ

2020 р.

**Мета роботи –** ознайомитись з основними принципами розкладання числа на прості множники з використанням різних алгоритмів факторизації.

**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.

**Завдання на лабораторну роботу**

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

**Лістинг програми:**

**MainActivity.java**

**package** com.example.rts\_lab31factorization;  
  
**import** androidx.appcompat.app.AppCompatActivity;  
**import** android.view.View;  
**import** android.os.Bundle;  
**import** android.widget.EditText;  
**import** android.widget.TextView;  
  
**public class** MainActivity **extends** AppCompatActivity {  
  
 @Override  
 **protected void** onCreate(Bundle savedInstanceState) {  
 **super**.onCreate(savedInstanceState);  
 setContentView(R.layout.***activity\_main***);  
 }  
 **public void** onButtonClick(View v){  
 EditText el\_n = (EditText)findViewById(R.id.***editText***);  
 TextView result1 = (TextView)findViewById(R.id.***textView2***);  
 TextView result2 = (TextView)findViewById(R.id.***textView3***);  
  
 **int** n = Integer.*parseInt*(el\_n.getText().toString());  
 **int** x, y, p = 0, q = 0;  
 **boolean** check = **true**;  
 **double** counter = Math.*ceil*(Math.*sqrt*(n));  
 **while** (check == **true**) {  
 **if** ((Math.*sqrt*((counter\*counter - n)))%1 ==0) {  
 x = (**int**)counter;  
 y = (**int**)Math.*sqrt*((counter\*counter - n));  
 p = x - y;  
 q = x + y;  
 check = **false**;  
 }  
 counter++;  
 }  
 result1.setText(Integer.*toString*(p));  
 result2.setText(Integer.*toString*(q));  
 }  
}

**activity\_main.xml**

*<?***xml version="1.0" encoding="utf-8"***?>*<**androidx.constraintlayout.widget.ConstraintLayout xmlns:android="http://schemas.android.com/apk/res/android"  
 xmlns:app="http://schemas.android.com/apk/res-auto"  
 xmlns:tools="http://schemas.android.com/tools"  
 android:layout\_width="match\_parent"  
 android:layout\_height="match\_parent"  
 tools:context=".MainActivity"**>  
  
 <**Button  
 android:id="@+id/button"  
 android:layout\_width="wrap\_content"  
 android:layout\_height="wrap\_content"  
 android:layout\_marginTop="68dp"  
 android:onClick="onButtonClick"  
 android:text="Розрахувати"  
 app:layout\_constraintEnd\_toEndOf="parent"  
 app:layout\_constraintStart\_toStartOf="parent"  
 app:layout\_constraintTop\_toBottomOf="@+id/editText"** />  
  
 <**EditText  
 android:id="@+id/editText"  
 android:layout\_width="wrap\_content"  
 android:layout\_height="wrap\_content"  
 android:layout\_marginTop="157dp"  
 android:ems="10"  
 android:hint="Введіть n"  
 android:inputType="number"  
 app:layout\_constraintEnd\_toEndOf="parent"  
 app:layout\_constraintStart\_toStartOf="parent"  
 app:layout\_constraintTop\_toTopOf="parent"** />  
  
 <**TextView  
 android:id="@+id/textView2"  
 android:layout\_width="wrap\_content"  
 android:layout\_height="wrap\_content"  
 android:layout\_marginBottom="75dp"  
 app:layout\_constraintBottom\_toTopOf="@+id/textView3"  
 app:layout\_constraintStart\_toStartOf="@+id/textView3"** />  
  
 <**TextView  
 android:id="@+id/textView3"  
 android:layout\_width="wrap\_content"  
 android:layout\_height="wrap\_content"  
 android:layout\_marginBottom="196dp"  
 app:layout\_constraintBottom\_toBottomOf="parent"  
 app:layout\_constraintEnd\_toEndOf="parent"  
 app:layout\_constraintStart\_toStartOf="parent"** />  
  
 <**TextView  
 android:id="@+id/P"  
 android:layout\_width="wrap\_content"  
 android:layout\_height="wrap\_content"  
 android:text="P = "  
 app:layout\_constraintBaseline\_toBaselineOf="@+id/textView2"  
 app:layout\_constraintEnd\_toEndOf="@+id/Q"  
 app:layout\_constraintStart\_toStartOf="@+id/Q"** />  
  
 <**TextView  
 android:id="@+id/Q"  
 android:layout\_width="wrap\_content"  
 android:layout\_height="wrap\_content"  
 android:layout\_marginStart="81dp"  
 android:layout\_marginLeft="81dp"  
 android:text="Q = "  
 app:layout\_constraintBaseline\_toBaselineOf="@+id/textView3"  
 app:layout\_constraintStart\_toStartOf="parent"** />  
  
</**androidx.constraintlayout.widget.ConstraintLayout**>

**Результат програми:**

