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:

студент групи ІП-84

Кабір Лабіб Ахмед

номер залікової книжки: 8416

Перевірив:

ас. Регіда П. Г.

Київ 2020

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.

Рис1. Алгоритми факторизації

Код програми

MainActivity.java

```
package com.example.lab31;

import android.annotation.SuppressLint;
import android.support.v7.app.AppCompatActivity;
import android.os.Bundle;
import android.view.View;
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);
   }

   @SuppressLint("SetTextI18n")
   public void Calculate(View view) {
      EditText editText = findViewById(R.id.edit_message);
      TextView textView = findViewById(R.id.textView);
      if(editText.getText().toString().equals("")) {
         textView.setText("Input number!");
         return;
      }
      int num = Integer.parseInt(editText.getText().toString());
      if(num == 0) {
         textView.setText("Incorrect number!");
         return;
      }

      double start = System.nanoTime();

      if(num % 2 == 0) {
         textView.setText(num + " = " + 2 + " * " + num / 2);
      } else {
         int x = (int) Math.sqrt(num);
         if (num == x * x) {
            textView.setText(num + " = " + x + " * " + x);
         } else {
            for (int i = 0; i < 10; i++){
               x++;
               double y = Math.sqrt(Math.pow(x, 2) - num);
               if (y % 1 == 0) {
                  textView.setText(num + " = " + (x - (int) y) + " * " + (x + (int) y) +
                        "\n" + "Time = " + (System.nanoTime() - start)/1000000 + " ms\n");
                  return;
               }
            }
            textView.setText("Error: Time exhausted!");
         }
      }
   }
}
```

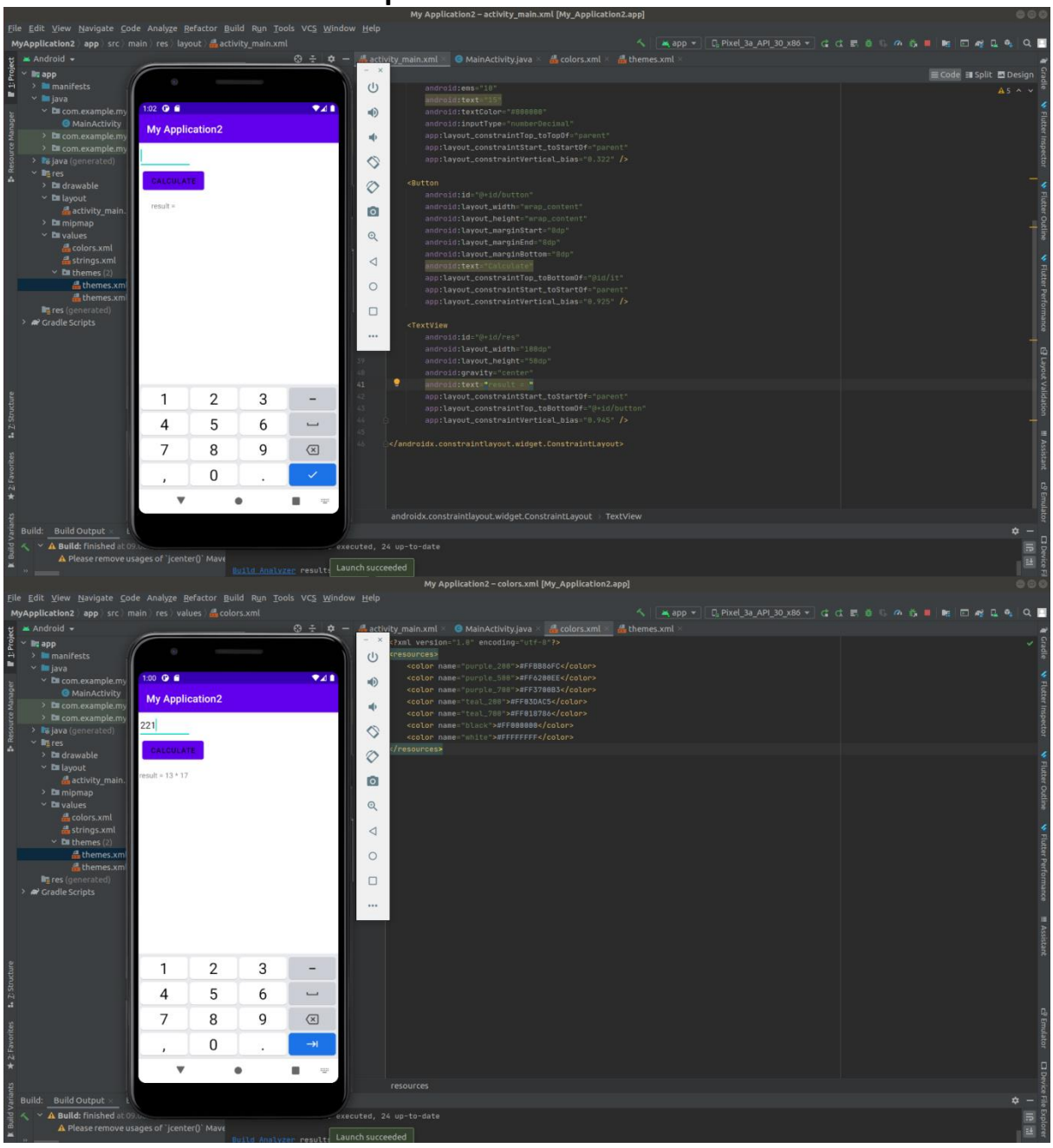
activity_main.xml

```
<?xml version="1.0" encoding="utf-8"?>
<android.support.constraint.ConstraintLayout
xmlns:android="http://schemas.android.com/apk/res/android"
```

```
xmlns:tools="http://schemas.android.com/tools"
android:layout_width="match_parent"
android:layout_height="match_parent"
android:background="#66CDAA"
android:orientation="horizontal"
tools:context=".MainActivity">

<LinearLayout
    android:layout_width="match_parent"
    android:layout_height="wrap_content"
    android:orientation="vertical"
    android:gravity="center"
    tools:ignore="MissingConstraints">

    <EditText
        android:id="@+id/edit_message"
        android:layout_width="wrap_content"
        android:layout_height="0dp"
        android:layout_weight="1"
        android:layout_marginTop="50dp"
        android:autofillHints="257"
        android:inputType="number"
        android:maxLength="9"
        android:hint="@string/input_number" />

    <Button
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:onClick="Calculate"
        android:text="@string/calculate"
        android:layout_marginTop="50dp"
        tools:ignore="MissingConstraints,OnClick" />

    <TextView
        android:id="@+id/textView"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:autoLink="web"
        android:linksClickable="true"
        android:layout_marginTop="50dp"
        android:textSize="20sp"
        tools:ignore="MissingConstraints" />

</LinearLayout>
```

```
</android.support.constraint.ConstraintLayout>
```

Скріншоти



Висновок

У цій роботі я дослідив основні принципи використання алгорутму факторизації. Я розробив програму на основі алгоритму Ферма за допомогою Flutter Dart.