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 №1-a**

«РЕАЛІЗАЦІЯ ЗАДАЧІ РОЗКЛАДАННЯ ЧИСЛА НА ПРОСТІ

МНОЖНИКИ (ФАКТОРИЗАЦІЯ ЧИСЛА)»

**Виконав:**

студент II курсу ФІОТ

групи ІВ-91

Бурбело Сергій

**Перевірив:**

Регіда П.Г.

Київ – 2021

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

**Завдання на лабораторну роботу:**

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

**Теоретичні відомості:**

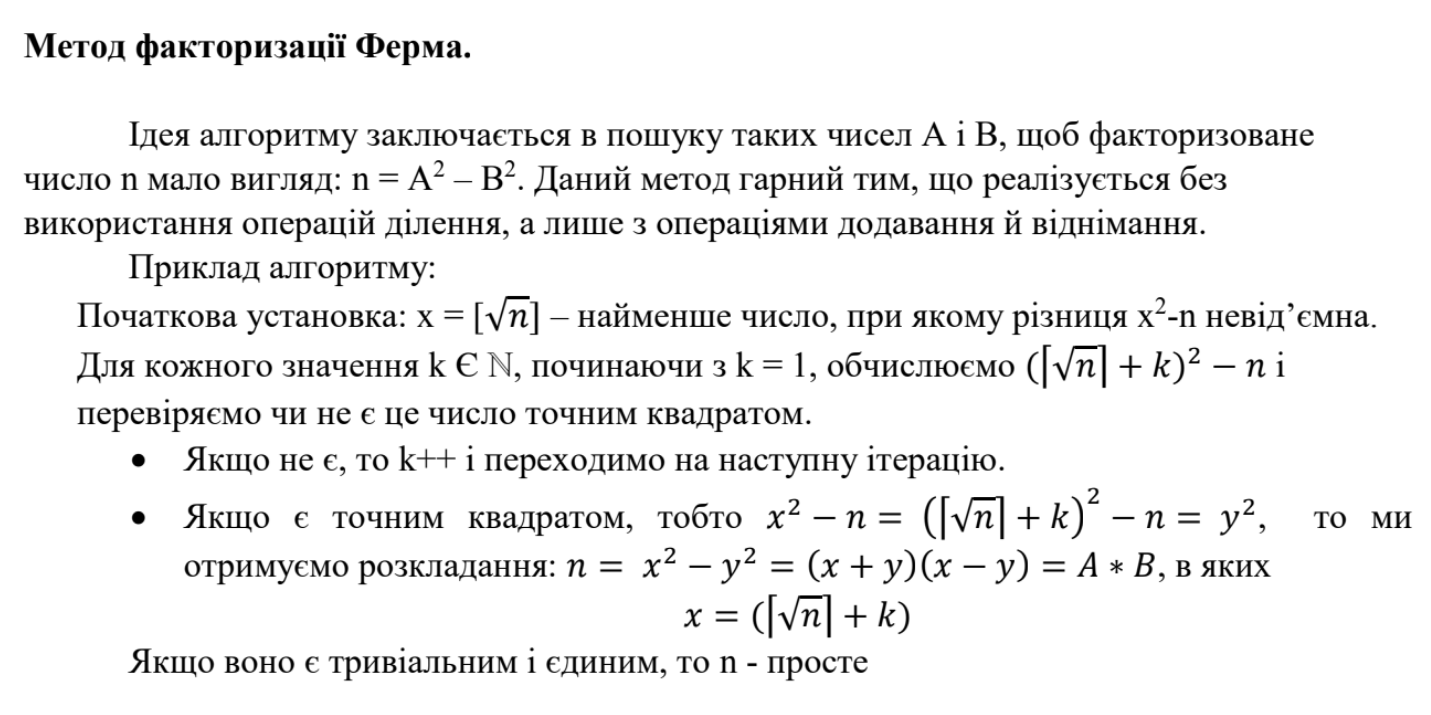
Факторизації лежить в основі стійкості деяких криптоалгоритмів, еліптичних кривих, алгебраїчній теорії чисел та кванових обчислень, саме тому дана задача дуже гостро досліджується, й шукаються шляхи її оптимізації.

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.

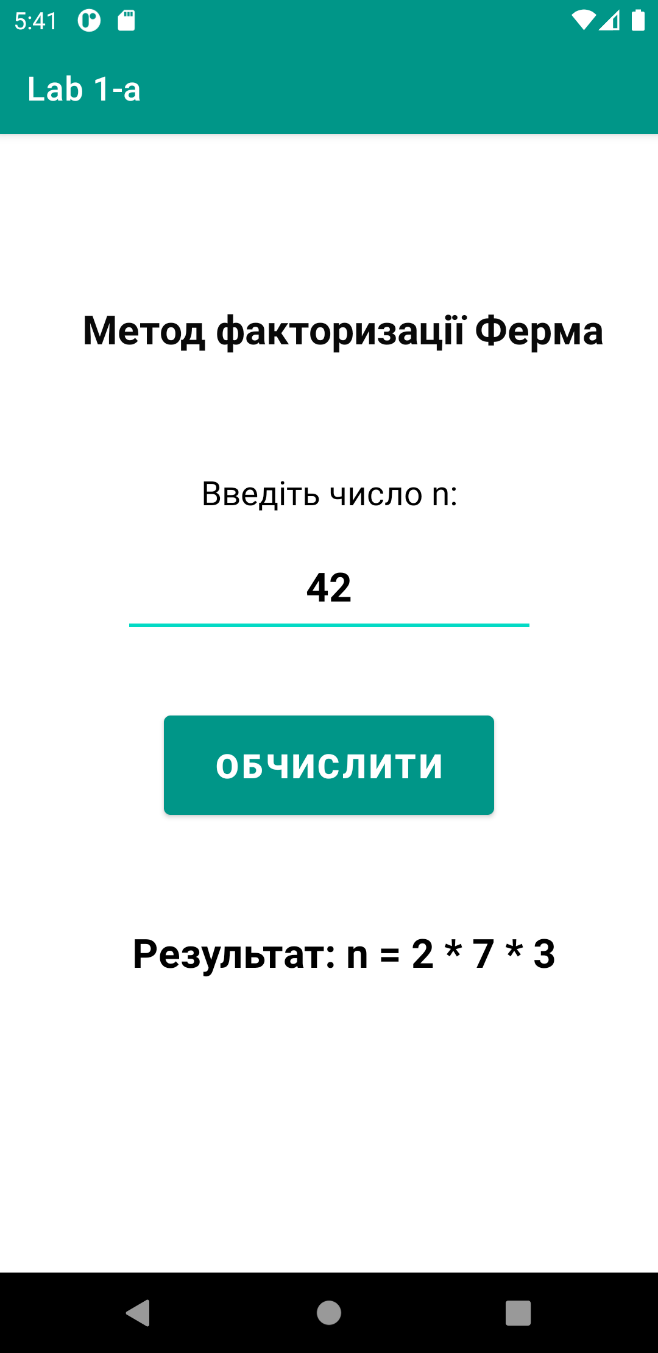


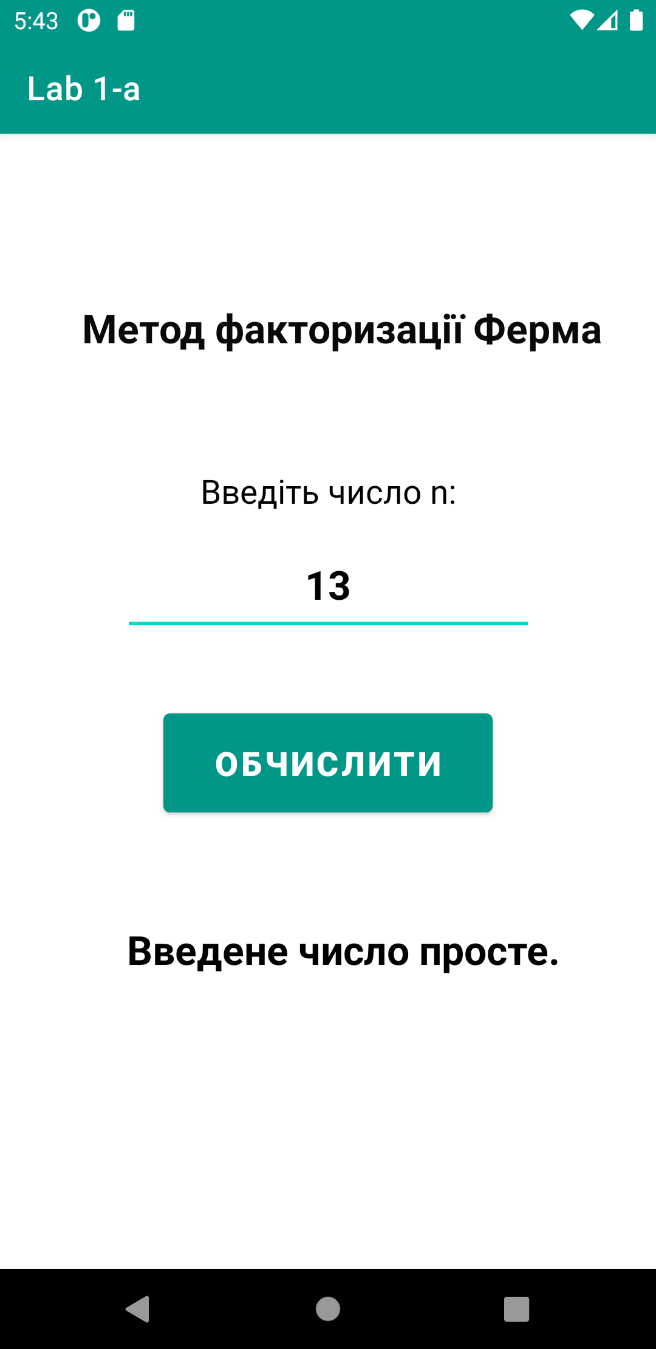
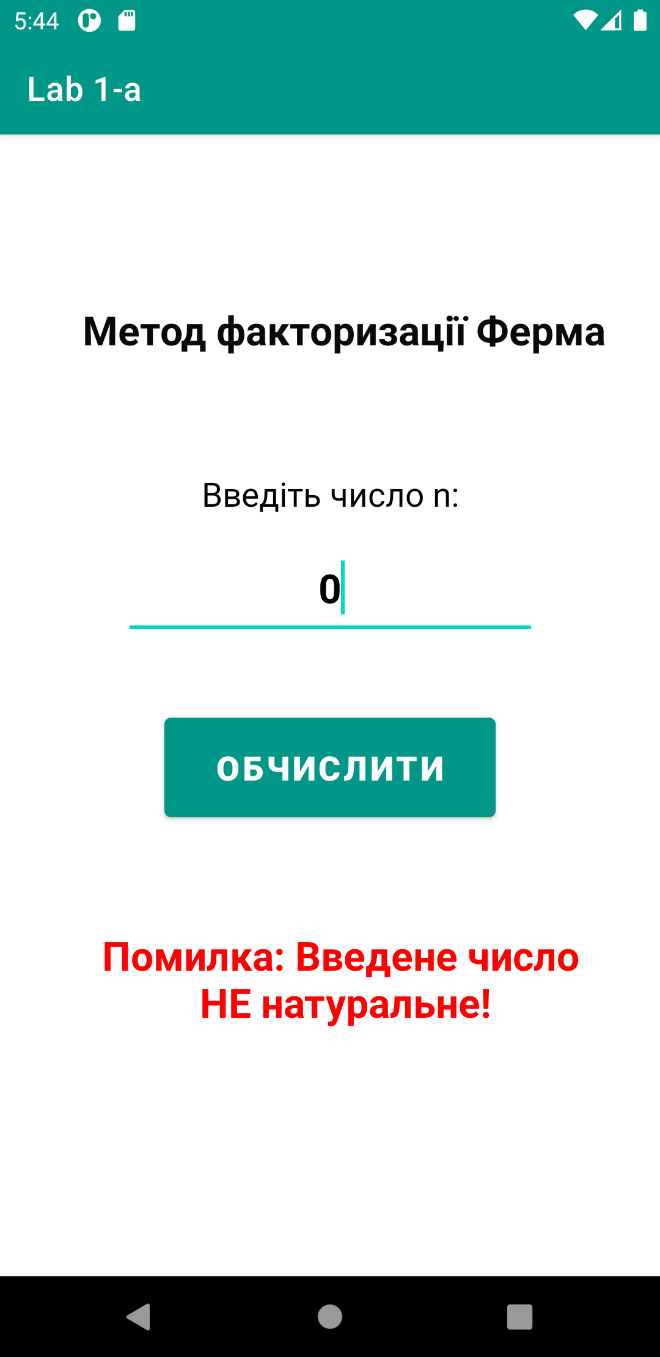
**Роздруківка тексту програми:**

package com.example.lab1\_a;  
  
import androidx.appcompat.app.AppCompatActivity;  
  
import android.os.Bundle;  
import android.content.Intent;  
import android.view.View;  
import android.widget.Button;  
  
public class MainActivity extends AppCompatActivity {  
  
 private Button btn\_1;  
  
 @Override  
 protected void onCreate(Bundle savedInstanceState) {  
 super.onCreate(savedInstanceState);  
 setContentView(R.layout.*activity\_main*);  
  
 this.btn\_1 = (Button) this.findViewById(R.id.*btn\_1*);  
  
 btn\_1.setOnClickListener(new Button.OnClickListener() {  
  
 @Override  
 public void onClick(View v) {  
  
 Intent myIntent = new Intent(MainActivity.this, Activity2.class);  
 MainActivity.this.startActivity(myIntent);  
 }  
 });  
 }  
}

package com.example.lab1\_a;  
  
import android.os.Bundle;  
import androidx.appcompat.app.AppCompatActivity;  
import android.view.View;  
import android.widget.Button;  
import android.widget.EditText;  
import android.widget.TextView;  
import java.util.ArrayList;  
import java.util.List;  
  
  
public class Activity2 extends AppCompatActivity {  
  
 EditText inputN;  
 Button btnResult;  
 TextView labelResult;  
  
 @Override  
 protected void onCreate(Bundle savedInstanceState) {  
 super.onCreate(savedInstanceState);  
 setContentView(R.layout.*activity\_2*);  
  
 this.inputN = this.findViewById(R.id.*enter\_n*);  
 this.btnResult = this.findViewById(R.id.*btn\_result*);  
 this.labelResult = this.findViewById(R.id.*label\_result*);  
  
 View.OnClickListener onButtonCountClick = r -> {  
  
 String stringN = String.*valueOf*(inputN.getText());  
  
 if (stringN.trim().equals("0")) {  
  
 labelResult.setTextColor(getResources().getColor(R.color.*error*));  
 labelResult.setText("Помилка: Введене число \nНЕ натуральне!");  
  
 } else if (stringN.trim().equals("")) {  
  
 labelResult.setTextColor(getResources().getColor(R.color.*error*));  
 labelResult.setText("Помилка: Не введені дані!");  
  
 } else {  
  
 long n = Long.*parseLong*(stringN);  
  
 Long[] multipliers = this.factors(n);  
  
 StringBuilder result = new StringBuilder("Результат: n = ");  
  
 for (int i = 0; i < multipliers.length - 1; i++) {  
 result.append(multipliers[i]).append(" \* ");  
 }  
  
 result.append(multipliers[multipliers.length - 1]);  
  
 if (multipliers[0] == n) {  
 result = new StringBuilder("Введене число просте.");  
 }  
 labelResult.setTextColor(getResources().getColor(R.color.*black*));  
 labelResult.setText(result);  
  
 }  
  
 };  
  
 btnResult.setOnClickListener(onButtonCountClick);  
 }  
  
 public Long[] factors(long n) {  
  
 List<Long> multipliers = new ArrayList<>();  
  
 while (n % 2 == 0) {  
  
 multipliers.add(2L);  
 n /= 2;  
  
 }  
  
 long[] sqrt = this.sumSqrt(n);  
 multipliers.add(Math.*abs*(sqrt[0] + sqrt[1]));  
 multipliers.add(Math.*abs*(sqrt[0] - sqrt[1]));  
  
 return multipliers.toArray(new Long[0]);  
  
 }  
  
 public long[] sumSqrt(long n) {  
  
 double x, y;  
  
 x = Math.*ceil*(Math.*sqrt*(n));  
 y = Math.*pow*(x, 2) - n;  
  
 while (Math.*sqrt*(y) != Math.*ceil*(Math.*sqrt*(y))) {  
  
 x++;  
 y = Math.*pow*(x, 2) - n;  
  
 }  
  
 return new long[]{(long) x, (long) Math.*sqrt*(y)};  
  
 }  
  
}

**Результати роботи програми:**

** **

** **

**Висновок:** У ході лабораторної роботи я ознайомився з основними принципами розкладання числа на прості множники з використанням різних алгоритмів факторизації. Був розроблений мобільний додаток під Android, що реалізує метод Ферма.