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 №1а

«РЕАЛІЗАЦІЯ ЗАДАЧІ РОЗКЛАДАННЯ ЧИСЛА НА ПРОСТІ МНОЖНИКИ (ФАКТОРИЗАЦІЯ ЧИСЛА)»

Виконав:
студент ІІ курсу ФІОТ
групи ІВ-91
Черних Богдан

Перевірив:
Регіда П.Г.

Київ – 2021

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

Теоретичі відомості

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 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: $x = \lceil\sqrt{n}\rceil$ – 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 до лабораторної роботи:

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

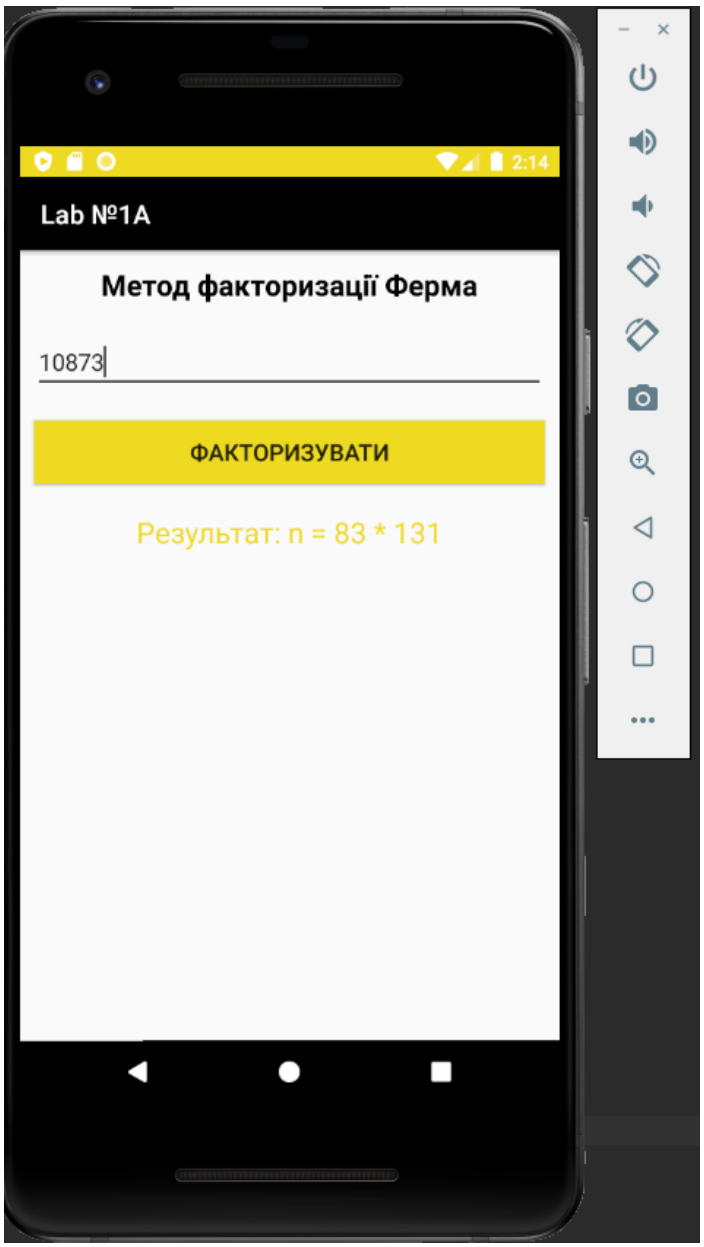
Роздруківка тексту програми

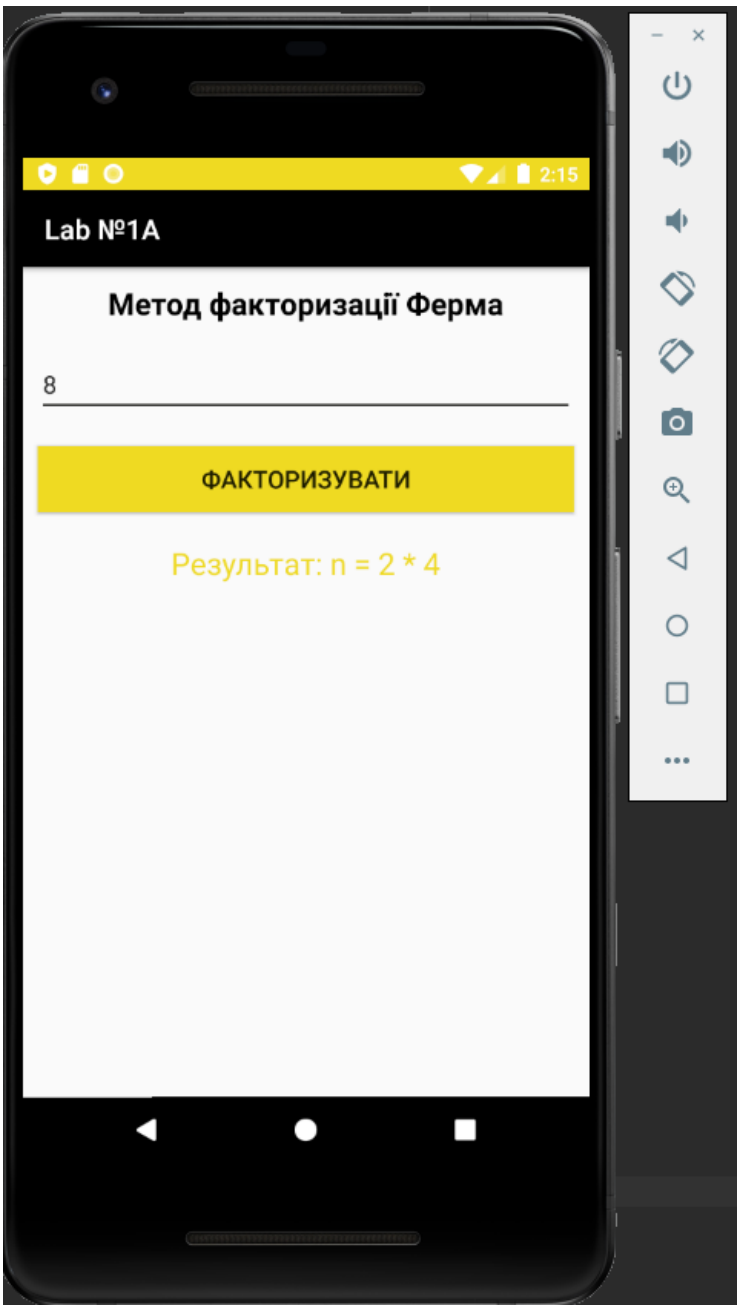
```
package com.example.lab1a;

import androidx.appcompat.app.AppCompatActivity;
```

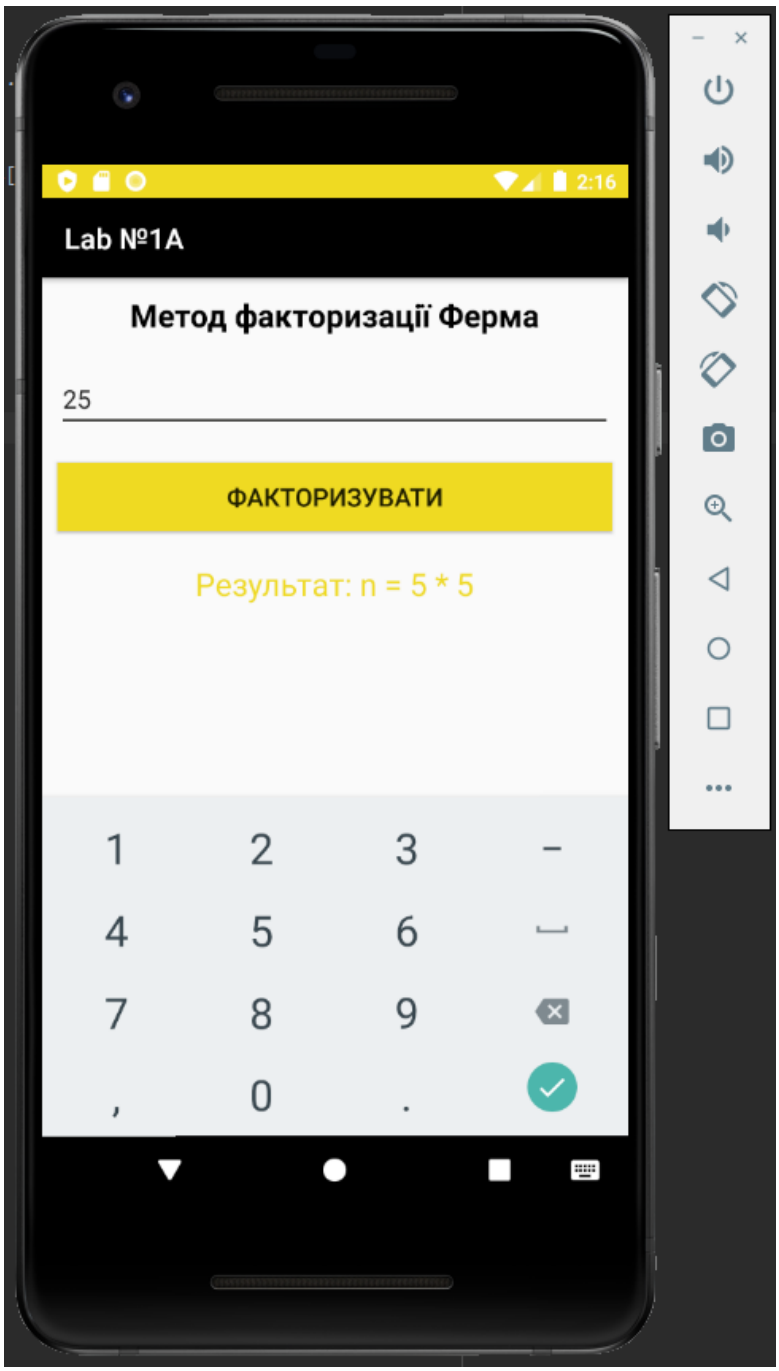
```java
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.TextView;

public class MainActivity extends AppCompatActivity {

    private EditText editText;
    private Button button;
    private TextView result;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        editText = findViewById(R.id.editTextNumber);
        button = findViewById(R.id.button);
        result = findViewById(R.id.result);

        button.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View view) {
                int n = Integer.parseInt(editText.getText().toString());
                FermMethod method = new FermMethod(n);
                int[] res = method.run();
                String resultText = "Результат: n = " + res[0] + " * " + res[1];
                result.setText(resultText);
            }
        });
    }
}

class FermMethod {

    public int n;
    public int[] result = new int [2];

    public FermMethod(int n) {
        this.n = n;
    }

    public int [] run() {
        int a = (int) Math.ceil(Math.sqrt(this.n));
        double b;

        // Якщо число є парним
        if (this.n % 2 == 0) {
            result[0] = 2;
            result[1] = this.n / 2;
            return result;
        }

        // Якщо число є точним квадратом
        if (a * a == this.n) {
            result[0] = a;
            result[1] = a;
            return result;
        }
```

```
        while (true) {
            double tmp = (a * a) - this.n;
            b = (int) Math.sqrt(tmp);

            if (b * b == tmp) {
                break;
            }
            a++;
        }

        result[0] = (int) (a - b);
        result[1] = (int) (a + b);
        return result;
    }
}
```

Результати роботи програми




2:15
Lab №1A
Метод факторизації Ферма
8
ФАКТОРИЗУВАТИ
Результат: n = 2 * 4



Висновок:

У ході лабораторної роботи я ознайомився з основними принципами розкладання числа на прості множники з використанням різних алгоритмів факторизації. Безпосередньо реалізував метод факторизації Ферма за допомогою мови програмування Java, після чого було розробленно мобільний додаток у Android Studio для візуалізації даних. В результаті проведення декількох перевірок, переконався в тому, що додаток працює належним чином та отриманий результат факторизації відповідає очікуваному результату. Таким чином, мета лабораторної роботи досягнута, про що засвідчують вищенаведені результати.