

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

ЛАБОРАТОРНА РОБОТА № 3_1

з дисципліни «Методи оптимізації та планування експерименту» на тему
«Реалізація задачі розкладання числа на прості множники
(факторизація числа)»

Виконав:
студент II курсу ФІОТ
групи ІО-93
Бриль Владислав

Перевірів:
Асистент Регіда П.Г.

Лабораторна робота 3_1

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

Завдання

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

Теоретичні відомості

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 $k \in \mathbb{N}$, 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

Виконання роботи

Код програми:

```
package com.lab1a.execution;

import java.util.ArrayList;
import java.util.List;

// Факторизація числа методом Ферма
public class Factorization {

    public static Long[] factorize(long n) {

        List<Long> multipliers = new ArrayList<>();

        while (n % 2 == 0) {
            multipliers.add(2L);
            n /= 2;
        }

        long[] sqrts = Factorization.getSumOfSquares(n);
        multipliers.add(Math.abs(sqrts[0] + sqrts[1]));
        multipliers.add(Math.abs(sqrts[0] - sqrts[1]));

        return multipliers.toArray(new Long[0]);
    }

    private static long[] getSumOfSquares(long n) {

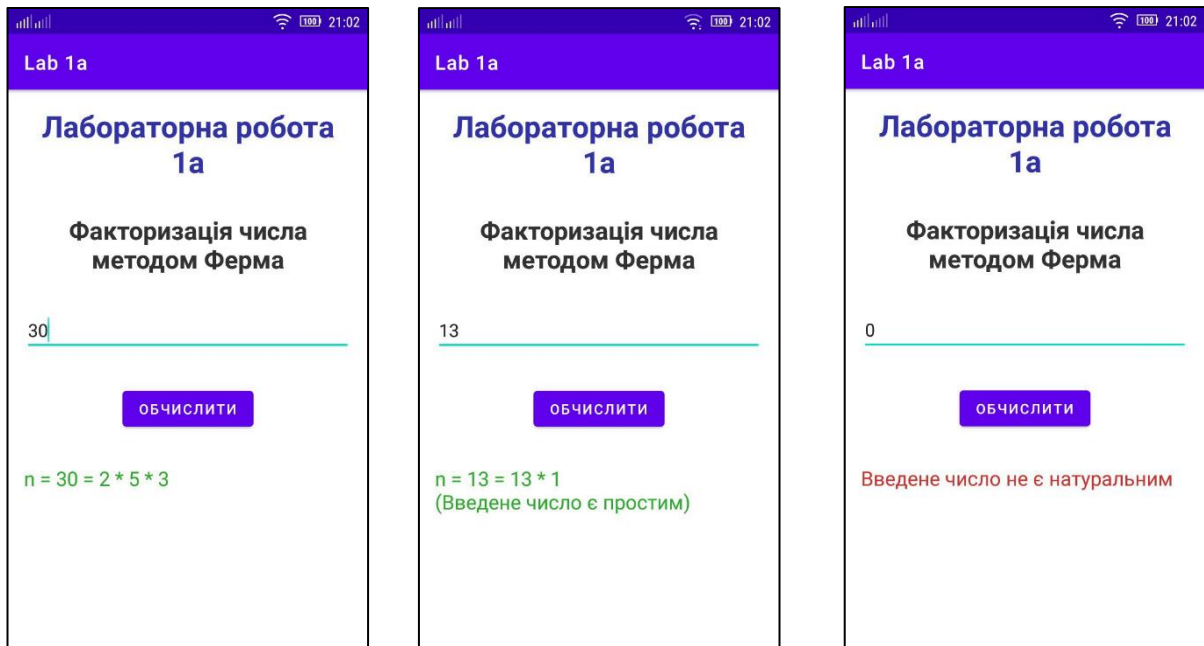
        double x, y;

        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



Висновок

При виконанні даної лабораторної роботи було вивчено основні принципи розкладання числа на прості множники з використанням різних алгоритмів факторизації. У ході роботи було розроблено програму для факторизації заданого числа методом Ферма.