

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 № 1а

з дисципліни «Методи планування експерименту»

на тему «Реалізація задачі розкладання числа на прості множники
(факторизація числа)»

Виконав:
студент 2 курсу
групи ІВ-92
Дмитришин А. Д.
Номер у списку групи: 6

ПЕРЕВІРИВ:
ас. Регіда П.Г.

Хід роботи

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

Основні теоретичні відомості, необхідні для виконання лабораторної роботи.

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

Завдання на лабораторну роботу

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

Лістинг

```
package com.example.mndlab1;

import ...

public class MainActivity extends AppCompatActivity {

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

    public void ferma(View view) {
        EditText edNumber = findViewById(R.id.editTextNumber);
        TextView tw = findViewById(R.id.textView2);
        int number = Integer.parseInt(edNumber.getText().toString());
        String ans = "";
        while (number % 2 == 0) {
            ans += 2 + " ";
            number /= 2;
        }
        if (isSimple(number)) {
            ans += number;
        } else ans += factorize(number);
        tw.setText(ans);
    }

    public static boolean perfectSquare(int x) {
        return Math.pow((int) Math.sqrt(x), 2) == x;
    }

    public static String factorize(int number) {
        int x = (int) Math.ceil(Math.sqrt(number));
        String ans = "";
        while (!perfectSquare(x * x - number)) {
            x += 1;
        }
        int y = (int) Math.sqrt(x * x - number);

        int[] s = {x - y, x + y};
        if (isSimple(s[0])) {
            ans += s[0] + " ";
        } else ans += factorize(s[0]);

        if (isSimple(s[1])) {
            ans += s[1] + " ";
        } else ans += factorize(s[1]);
        return ans;
    }

    public static boolean isSimple(int num) {...}
}
```

Результати роботи програми

