# 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-а

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

#### Виконав:

студент II курсу ФІОТ групи IB-93 Гордійчук Юрій

#### Перевірив:

Регіда П.Г.

**Мета роботи:** Ознайомитись 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  $n \in \mathbb{N}$ , 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:

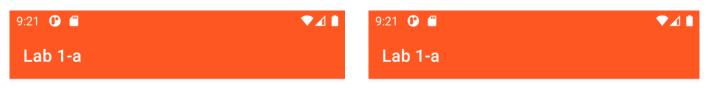
Початкова установка:  $\mathbf{x} = [\sqrt{n}]$  — найменше число, при якому різниця  $\mathbf{x}^2$ -п невід'ємна. Для кожного значення  $\mathbf{k} \in \mathbb{N}$ , починаючи з  $\mathbf{k} = 1$ , обчислюємо  $(\sqrt[]{n} + k)^2 - n$  і перевіряємо чи не  $\epsilon$  це число точним квадратом.

- Якщо не  $\epsilon$ , 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

#### Роздруківка тексту програми:

#### Результати роботи програми:



# Лабораторна робота №1а

# Лабораторна робота №1а

Факторизація числа методом Ферма

Факторизація числа методом Ферма

Введіть число = 66

Введіть число = 13

обчислити

обчислити

Відповідь: n = 2 \* 11 \* 3

Введене число просте.





## Лабораторна робота №1а

Факторизація числа методом Ферма

Введіть число = 0

обчислити

Введене число НЕ натуральне!

# Лабораторна робота №1а

Факторизація числа методом Ферма

Введіть число = 33

обчислити

Відповідь: n = 11 \* 3



## Лабораторна робота №1а

Факторизація числа методом Ферма

Введіть число = 15

ОБЧИСЛИТИ

Відповідь: n = 5 \* 3

**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.