МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФАКУЛЬТЕТ ІНФОРМАТИКИ ТА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ
КАФЕДРА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Лабораторна робота №3.1
з дисципліни «Інтелектуальні вбудовані системи»

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

Виконав:
студент гр. ІП-84
Дмитренко Олександр

Перевірив:
Регіда П.Г.

Київ 2021

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: $x = [\sqrt{n}]$ – 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 $x^2 - n = \left(\lceil\sqrt{n}\rceil + k\right)^2 - n = y^2$, 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

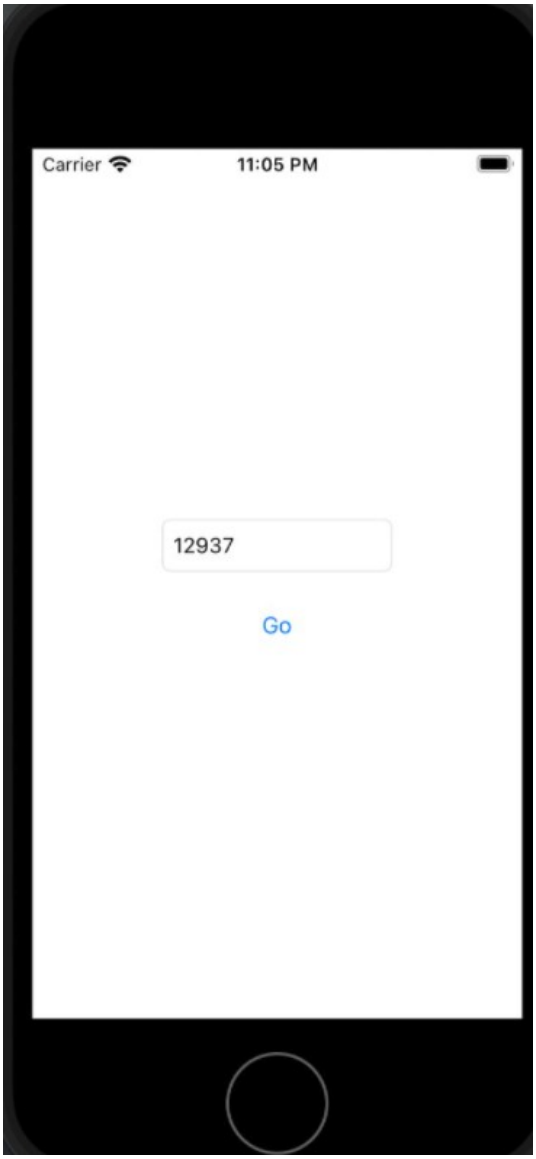
Завдання

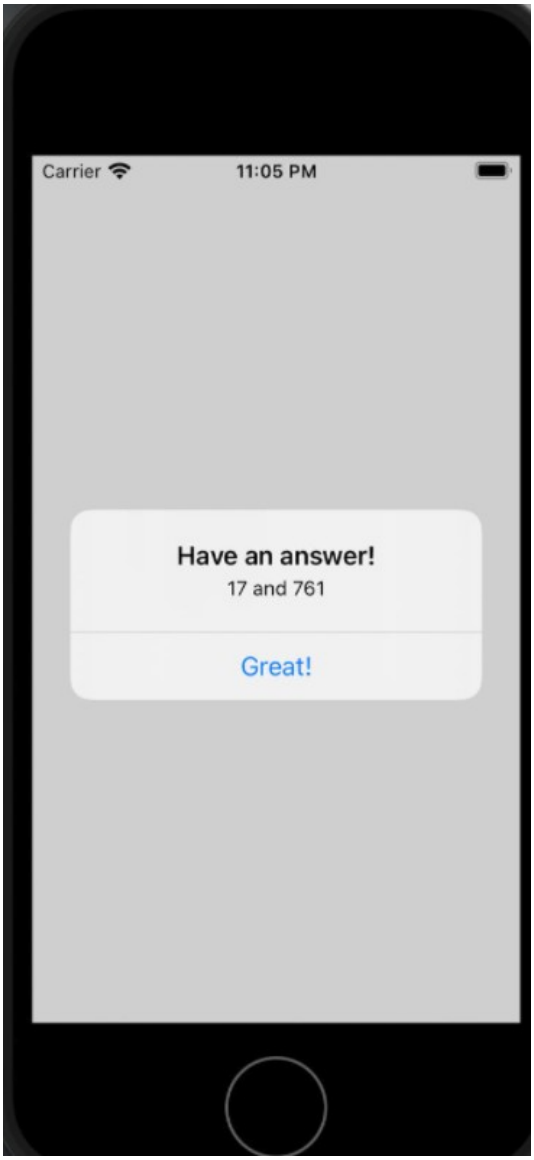
Розробити програма для факторизації заданого числа методом Ферма. Реалізувати користувацький інтерфейс з можливістю вводу даних.

Лістинг програми

```swift
//
//  ViewController.swift
//  lab1
//
//  Created by Sasha Dmytrenko on 5/22/21.
//

import UIKit

class ViewController: UIViewController {

    @IBOutlet weak var textField: UITextField!

    @IBAction func goButtonTapped(_ sender: Any) {
        textField.resignFirstResponder()
        guard let value = textField.text,
              let number = Int(value) else {
            return
        }

        guard let (x, y) = fermatFactor(of: number) else {
            return
        }

        let ac = UIAlertController(title: "Have an answer!", message: "\(x) and \(y)", preferredStyle: .alert)
        ac.addAction(UIAlertAction(title: "Great!", style: .default))

        present(ac, animated: true)
    }

    func fermatFactor(of n: Int) -> (Int, Int)? {

        if n <= 0 {
            return nil
        }

        if n.isMultiple(of: 2) {
            return (2, n / 2)
        }

        var a = Int(Double(n).squareRoot().rounded(.up))
        var b2 = a * a - n

        while !b2.isSquare() {
            a = a + 1
            b2 = a * a - n
        }
        let x = a - Int(Double(b2).squareRoot().rounded(.up))
        return (x, n / x)

    }

}

extension Int {

    func isSquare() -> Bool {
        let root = Int(Double(self).squareRoot())
        return root * root == self
    }

}
```

Результат роботи програми





Висновки

Під час виконання лабораторної роботи було досліджено метод факторизації числа Ферма. Реалізовано програму з користувацьким інтерфейсом, яка б розкладала числа на прості множники та виводила їх на екран.