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 №3.1
з дисципліни
«Інтелектуальні вбудовані системи»
на тему
«РЕАЛІЗАЦІЯ ЗАДАЧІ РОЗКЛАДАННЯ ЧИСЛА НА ПРОСТІ МНОЖНИКИ (ФАКТОРИЗАЦІЯ ЧИСЛА)»

Виконав:
студент групи ІП-84
Гудь В.В.
№ залікової книжки: ІП-8405

Перевірив:
викладач
Регіда П.Г.

Київ 2021

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 $x^2 - n = (\lceil\sqrt{n}\rceil + k)^2 - n = y^2$, 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.

Вихідний код

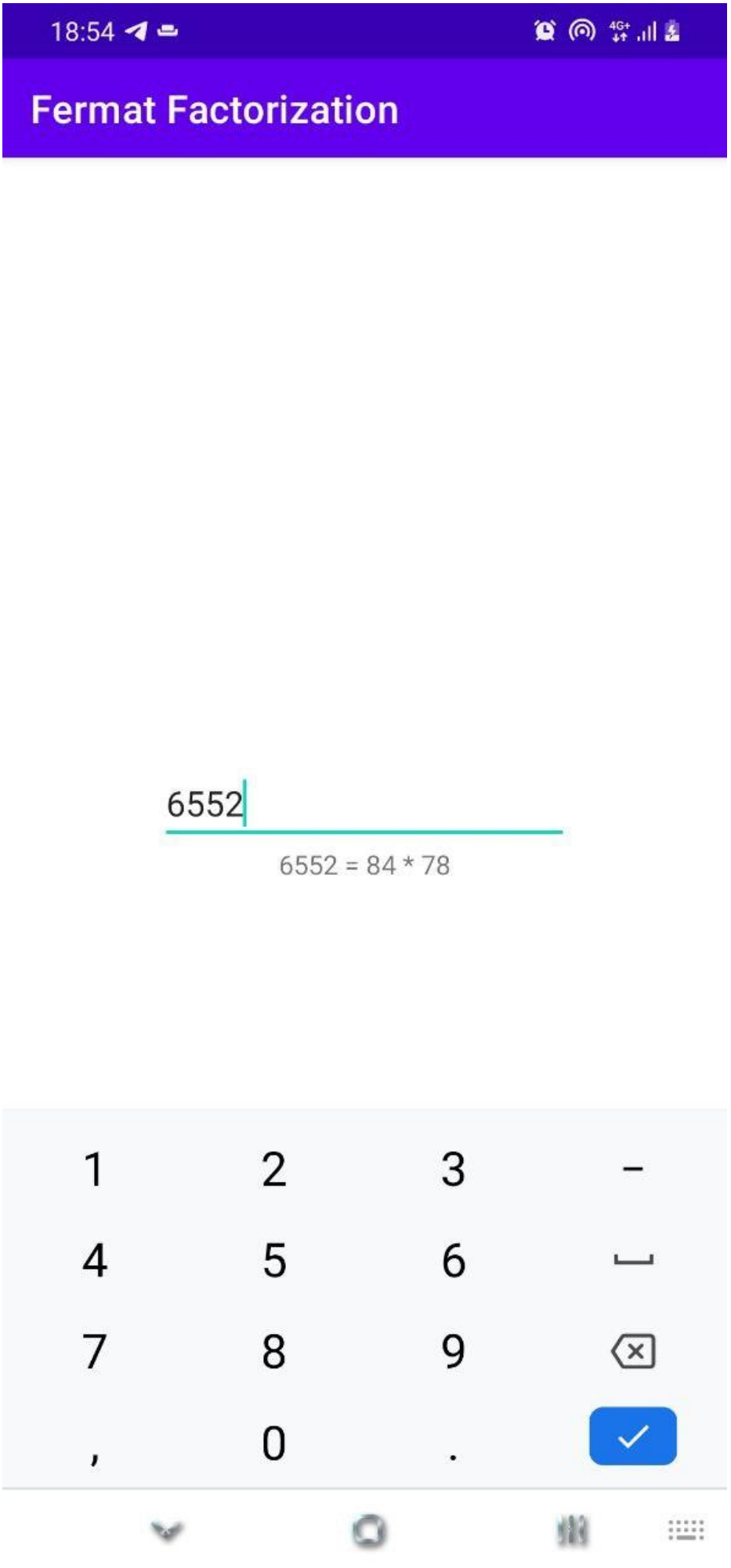
```
private fun fermatFactorization(number: Long, textView: TextView) {
    GlobalScope.launch(Dispatchers.IO) {
        try {
            val res = factorize(number).joinToString(" * ")
            withContext(Dispatchers.Main) {
                textView.text = "$number = $res"
            }
        } catch (e: IllegalStateException) {
            withContext(Dispatchers.Main) {
```

```
                Toast.makeText(applicationContext, "${e.message}",
Toast.LENGTH_SHORT).show()
            }
        }
    }
}

private fun factorize(number: Long) : List<Long> {
    if (number <= 0) error("Cannot factorize non-positive numbers")
    var root = ceil(sqrt(number.toFloat())).toLong()
    if (root * root == number) return listOf(root, root)
    while (root != (number + 1) / 2) {
        val r = root * root - number
        val perfectSqrt = isPerfectSquare(r)
        if (perfectSqrt != -1L) {
            return listOf(root + perfectSqrt, root - perfectSqrt)
        }
        ++root
    }
    error("Cannot factorize $number")
}

private fun isPerfectSquare(num: Long) : Long {
    val sqrt = sqrt(num.toFloat())
    if (ceil(sqrt) == sqrt) return sqrt.toLong()
    return -1
}
```

Результати роботи програми


18:54
Fermat Factorization
6552
6552 = 84 * 78
1
2
3
4
5
6
7
8
9
,
0
.

Висновки

Під час даної лабораторної роботи розробили програму для факторизації чисел та користувацький інтерфейс з можливістю вводу даних.

.