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

Валигні Андрій Олексвндрович
номер залікової книжки: 8503

Перевірив:

ас. Регіда П. Г.

Київ 2020

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

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.

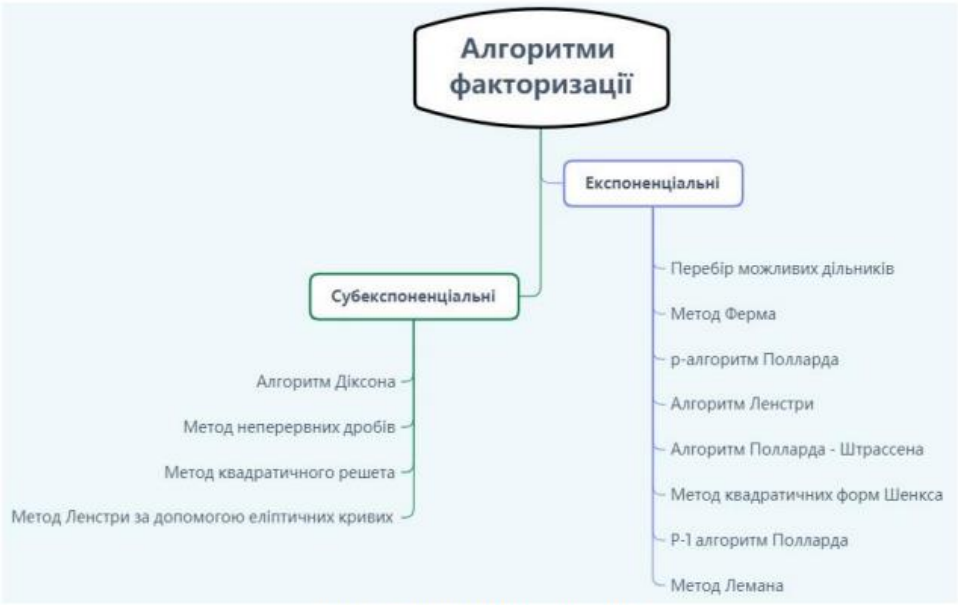


Рис1. Алгоритми факторизації

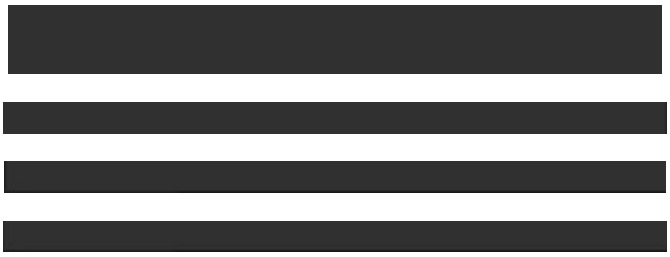
Код програми

```
import 'dart:math';



ferma(int n) {
  if (n < 0) return 'must be > 0';
  if (n % 2 == 0) return 'is not odd';
  int x = sqrt(n).toInt();
  int y = 0;
  while (true) {
    int r = (x * x) - n;
    if (r > 0) {
      y = sqrt(r).toInt();
    }
    if ((y * y) == r) {
      int a = x - y;
      int b = x + y;
      return '$a * $b = $n';
    }
    x++;
  }
}
```

Скріншоти



Висновок

У цій роботі я дослідив основні принципи використання алгорутму факторизації. Я розробив програму на основі алгоритму Ферма за допомогою Flutter Dart.