Лабораторна робота №1
з предмету
Теоретико числові алгоритми

Роботу виконала:
Бекешева Анастасія
3-го курсу
групи ФІ-12

Приймав:
Якимчук Олексій

1 Мета.

Практичне ознайомлення з різними методами факторизації чисел, реалізація цих методів і їх п рівняння. Виділення переваг, недоліків та особливостей застосування алгоритмів факторизації. Застосування комбінації алгоритмів факторизації для пошуку канонічного розкладу заданого числа.

2 Постановка задачі та варіант завдання.

Пошук канонічного розкладу великого числа, використовуючи відомі методи факторизації, а також особлива увага алгоритму Брілхарта-Моррісона. Варіант 1.

3 Хід роботи.

3.1 План.

1. Створення github repo.
2. Імплементація імовірнісного тесту Соловея-Штрассена.
3. Імплементація методу проблих ділень.
4. Імплементація ρ-методу Полларду.
5. Імплементація (багатомученна) Бріллхарта-Моррісона.
6. Підняття Docker.

3.2 Проблеми.

В БМ були проблеми з генеруванням гладних чисел, бо в ідеалі треба ланцюговий дріб генерувати поки не вистачить гладких чисел, а в методі ну трохи не так описано, звісно до цього я могла і сама догадатись, але щоб студенти в майбутньому менше мучались додайте цей пунктик в методу будь ласка :) Ну і власне я фіксила це вже поверх купи написаного коду, тому воно костильне, але як мінімум на числах з дз працює.

4 Результати

```
   1495056764861639599 = 17 * 6871 * 853103 * 15003319
Elapsed time:  32.2915358543396 seconds.

   15196946347083 = 3 * 89 * 2297 * 24779017
Elapsed time:  4.913546800613403 seconds.

   61333127792637 = 3 * 89 * 2297 * 100005263
Elapsed time:  6.326192855834961 seconds.

   17873 = 61 * 293
Elapsed time:  0.12788724899291992 seconds.
```

5 Висновки

В результаті виконання лабораторної роботи повторно ознайомилась з матеріалами з лекцій. Моя реалізація БМ не є дуже дієвою на великих числах через вище описану проблему. Але можу зазначити, що вийшло реалізувати швидкий розв'язок СЛР. В випадку з числами які мають декілька простих не дуже великих дільників комбінація методу пробних ділень та ρ-методу Полларда справляються непогано.