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

```
   901667173167834173 = 31 * 6211 * 316937 * 14775769
Elapsed time:  0.520775318145752 seconds.

   3009182572376191 = 30091489 * 100001119
Elapsed time:  8.92608904838562 seconds.

   1021514194991569 = 10214959 * 100001791
Elapsed time:  8.837704181671143 seconds.

   4000852962116741 = 40007321 * 100003021
Elapsed time:  53.757988691329956 seconds.
```

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

   15196946347083 = 3 * 89 * 2297 * 24779017
Elapsed time:  1.9654781818389893 seconds.

   499664789704823 = 15003319 * 33303617
Elapsed time:  1.6105360984802246 seconds.

   269322119833303 = 10868959 * 24779017
Elapsed time:  1.863227128982544 seconds.

   679321846483919 = 28065119 * 24205201
Elapsed time:  2.9098618030548096 seconds.

   96267366284849 = 962623 * 100005263
Elapsed time:  20.774596691131592 seconds.

   61333127792637 = 3 * 89 * 2297 * 100005263
Elapsed time:  17.09094500541687 seconds.

   2485021628404193 = 24849479 * 100002967
Elapsed time:  5.502688884735107 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.

6 Docker.

```
docker run bekeshevaaa/nta-lab-1:0.7 python3 script.py n
```