НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. СІКОРСЬКОГО»
НН ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1 З ПРЕДМЕТУ «ТЕОРЕТИКО-ЧИСЛОВІ АЛГОРИТМИ У КРИПТОЛОГІЇ»

«ПОШУК КАНОНІЧНОГО РОЗКЛАДУ ВЕЛИКОГО ЧИСЛА, ВИКОРИСТОВУЮЧИ ВІДОМІ МЕТОДИ ФАКТОРИЗАЦІЇ»

Виконали:
ФІ-04 Радомир Беш
ФІ-04 Давидюк Данил

Мета роботи

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

Постановка задачі та варіант завдання

1. Написати програми, що реалізовують такі алгоритми:
(а) один з тестів на простоту (*Міллера-Рабіна або Соловея-Штрассена*);
(б) *метод пробних ділень*;
(в) *ρ-метод Полларда*;
(г) *метод Брілхарта-Моррісона або метод Померанця.*
2. Створити та реалізувати алгоритм для пошуку канонічного розкладу числа, що використовує (всі) вищезгадані алгоритми. Цей алгоритм повинен повертати канонічний розклад числа. Кроки алгоритму наведено нижче. Додатково алгоритм повинен інформувати користувача про кожен дільник, знайдений в процесі роботи алгоритму, а саме: сам дільник; алгоритм, за допомогою якого було знайдено цей дільник; і часову відмітку, коли його було знайдено. Часові відмітки часу початку і кінця роботи алгоритму також повинні відображатися в цьому інформуванні.

(а) Вхід: n. Перевірити чи вхідне число n є простим. Якщо число є простим, то додати n до результату і завершити роботу, якщо число є складеним, перейти до наступного кроку.

(б) Вхід: n. Застосувати метод пробних ділень для пошуку дільників вхідного числа. Пробні ділення робити числами, що не перевищують 47. Якщо дільник a знайдено, записати його у вихідний результат і повернутися до кроку 3а з вхідним значенням n/a. Якщо дільник не знайдено перейти до кроку 3в.

(в) Вхід: n. Застосувати ρ-метод Полларда. Якщо дільник a знайдено, записати його у вихідний результат і перейти на крок 3г з числом n/a. Якщо дільник не знайдено перейти до кроку 3д.

(г) Вхід: n. Перевірити чи вхідне число є простим. Якщо число є простим, то додати n до результату і завершити роботу, якщо число є складеним, перейти до наступного кроку.

(д) Вхід: n. Застосувати метод Брілхарта-Моррісона або метод Померанця. Якщо дільник a знайдено, записати його у вихідний результат і повернутися на один крок назад з числом n/a. Якщо дільник не знайдено

завершити роботу з повідомленням "я не можу знайти канонічний розклад числа :(".

5. Застосувати алгоритм, створений на попередньому кроці, для пошуку канонічного розкладу числа відповідного варіанту №: 3

Число :
2500744714570633849

6. Застосувати реалізовані алгоритми факторизації (ρ-метод Полларда та метод Брілхарта-Моррісона (або метод Померанця)) почергово до всіх наступних чисел, знайти один дільник цього числа, заміряти час роботи кожного алгоритму на кожному числі, порівняти та пояснити результати.
Числа:
• 3009182572376191
• 1021514194991569
• 4000852962116741
• 15196946347083
• 499664789704823
• 269322119833303
• 679321846483919
• 96267366284849
• 61333127792637
• 2485021628404193

Хід роботи, опис труднощів, що виникали, та шляхів їх розв’язання

Наш шлях був складним та складеним , складним тому що було важко зробити те , на що надавалось декілька тижнів , а складеним , тому що скласти докупи всю необхідну інформацію було майже нереальною задачею.

Першим пунктом ми зробили ймовірнісний тест Міллера-Рабіна на простоту числа , реалізувавши функцію перевірки на псевдо простоту числа p.Ідея тесту полягає в тому, щоб перевіряти для випадково вибраних чисел a<n, чи є свідками простоти числа n. Якщо знайдеться свідок того, що число є складовим, то число дійсно є складовим. Якщо було перевірено k чисел, і вони виявилися свідками простоти, то число вважається простим. Для такого алгоритму ймовірність прийняти складову кількість за просте буде

менше (1/4)^k , що для навіть незначних значень k буде виправдовувати його застосування. Далі нас чекав політ фантазій з методом пробних ділень , він вийшов не занадто складним , але ми заплутались в типі даних , але згодом в нас вийшло , все зробити нормально. Аналогічно було з методом rho - Полларда , в ньому ми вирішили застосувати модифікацію Флойда , цей алгоритм типу Лас-Вегас , тому якщо він видає значення то воно точно правильне. І тут наша вдача закінчилась... З алгоритмом CFRAC ми так і не впорались , було багато спроб , багато крові , але не вийшло на жаль. Хоча наш алгоритм пробних ділень та rho -Полларда працює на ура. І може факторизовувати дуже великі числа. Нижче буде наведені скріни результату роботи алгоритму.

Згідно за 3 Варінтом :

```
dotnet run
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера
-Робіна:
Число 2500744714570633849 є складеним

Множники:
Дільник 43 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0071309
Дільник 7699 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0032681
Дільник 303983 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.1341880
Дільник 24849479 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.1062549

Дільники:
[43, 7699, 303983, 24849479]
```

Далі будуть наведені , результату обчислення інших чисел :

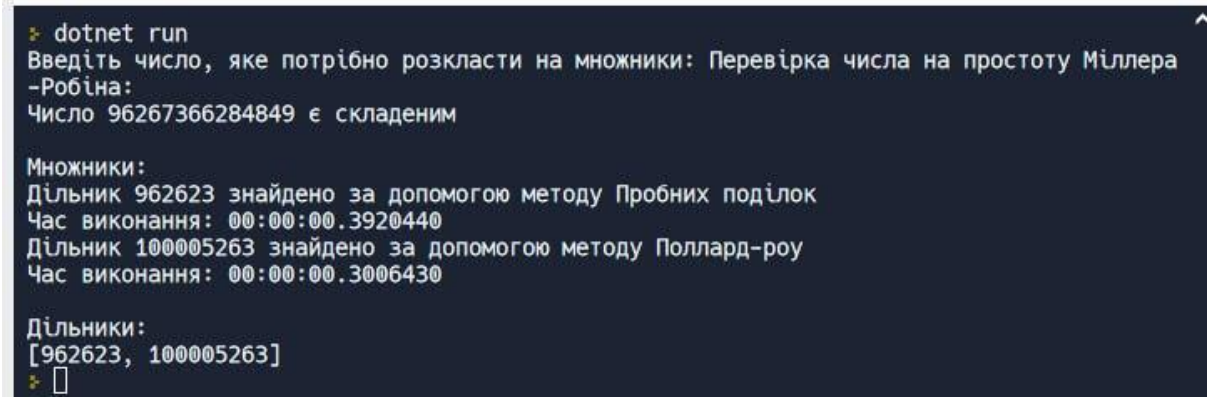
```
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Мі
-Робіна:
Число 3009182572376191 є складеним

Множники:
Дільник 30091489 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:24.8347283
Дільник 100001119 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.3674749

Дільники:
[30091489, 100001119]
```

```
> dotnet run
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера
-Робіна:
Число 1021514194991569 є складеним

Множники:
Дільник 10214959 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:08.9068553
Дільник 100001791 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.2094590

Дільники:
[10214959, 100001791]
>
```

```
> dotnet run
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера
-Робіна:
Число 4000852962116741 є складеним

Множники:
Дільник 40007321 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:38.1022603
Дільник 100003021 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:01.0140600

Дільники:
[40007321, 100003021]
```

```
> dotnet run
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера
-Робіна:
Число 499664789704823 є складеним

Множники:
Дільник 15003319 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:11.7980402
Дільник 33303617 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.1671819

Дільники:
[15003319, 33303617]
>
```

```
> dotnet run
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера
-Робіна:
Число 679321846483919 є складеним

Множники:
Дільник 24205201 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:20.5401165
Дільник 28065119 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.0654830

Дільники:
[24205201, 28065119]
```




```
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера-Робіна:
Число 61333127792637 є складеним

Множники:
Дільник 3 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0076502
Дільник 89 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0001100
Дільник 2297 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0022901
Дільник 100005263 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.5350816

Дільники:
[3, 89, 2297, 100005263]
```

```
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера-Робіна:
Число 2485021628404193 є складеним

Множники:
Дільник 24849479 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:24.5602176
Дільник 100002967 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.3061867

Дільники:
[24849479, 100002967]
```

```
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера-Робіна:
Число 269322119833303 є складеним

Множники:
Дільник 10868959 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:10.7589021
Дільник 24779017 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.1839940

Дільники:
[10868959, 24779017]
```

```
Введіть число, яке потрібно розкласти на множники: Перевірка числа на простоту Міллера-Робіна:
Число 15196946347083 є складеним

Множники:
Дільник 3 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0066801
Дільник 89 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0001200
Дільник 2297 знайдено за допомогою методу Пробних поділок
Час виконання: 00:00:00.0022800
Дільник 24779017 знайдено за допомогою методу Поллард-роу
Час виконання: 00:00:00.1829340

Дільники:
[3, 89, 2297, 24779017]
```

Результат бачимо , що для чисел виду pq алгоритм пробних ділень та rho - Поллард працює дуже швидко.

Висновки : У цій лабораторній роботі ми спробували реалізувати алгоритми факторизації великих чисел. В нас вийшла програмна реалізація методів

пробних ділень та rho -Полларда , але проблему з алгоритмом CFRAC в нас не вийшло подолати. Побачили , що алгоритми пробних ділень та rho -Полларда працює дуже швидко на великих числах виду pq. Вважаємо ,що ми набули значних навиків зі створення алгоритмів факторизації , які і надалі будемо використовувати в наступних проектах.