Лабораторна робота 1. (Довга арифметика)

Реалізувати довгу арифметику цілих чисел зі знаком:

1) Операції: додавання, віднімання, множення, ділення з залишком (підрахунок частки та залишку), піднесення до натурального степеня.
2) Порівняння чисел (<,>,=).
3) Ті ж самі операції (крім порівняння) за заданим модулем.
4) Знаходження $[\sqrt{x}]$, де $[x]$ позначає цілу частину $x \in Z$.
5) Розв'язання систем порівнянь першого порядку.

Умови:

- Мови програмування: C++, Java, Python і т.д.
  Якщо в обраній мові програмування реалізована довга арифметика, то відповідні функції застосовувати **заборонено.**
- Розрядність чисел **не** повинна бути обмежена наперед заданою програмною верхньою границею.
- Реалізувати лабораторну роботу у вигляді зовнішнього модуля, який можна було б застосовувати в інших додатках. Довга арифметика знадобиться в другій лабораторній роботі.

Лабораторна робота 2. (Основні алгоритми теорії чисел та криптографії)

Використовуючи модуль довгої арифметики з першої лабораторної роботи, реалізувати основні алгоритми криптографії та теорії чисел:

1) Один алгоритм факторизації довгих цілих чисел на вибір: ро-алгоритм Полларда або алгоритм квадратичного решета.
2) Один алгоритм знаходження дискретного логарифма на вибір: ро-алгоритм Полларда або алгоритм «великий крок – малий крок».
3) Обчислення функцій Ейлера та Мьобіуса.
4) Обчислення символів Лежандра та Якобі.
5) Алгоритм Чіпполи знаходження дискретного квадратного кореня.
6) Один алгоритм перевірки чисел на простоту на вибір: алгоритм Соловея-Штрассена або алгоритм Міллера-Рабіна.
7) Криптосистема Ель-Гамаля над еліптичними кривими.

Умови:

- Алгоритми реалізувати в довгій арифметиці.
- Для перевірки тестів на простоту використовувати таблиці довгих простих чисел, наприклад: https://primes.utm.edu/nthprime/index.php#nth
- Параметри для еліптичних кривих вибирати згідно з таблицями: http://www.secg.org/SEC2-Ver-1.0.pdf