Вспомогательные задания к работе №4 по фундаментальным алгоритмам.

1. Реализуйте класс длинного целого числа, предоставляющий следующий функционал:

   - сложение чисел;
   - вычитание чисел;
   - умножение чисел (в столбик);
   - Конструктор от строки с числом в заданной системе счисления (2 параметра, система счисления от 2 до 36);
   - Конструктор копирования;
   - Оператор присваивания;
   - Деструктор;
   - Перегруженный оператор вставки в поток;
   - Генерация псевдослучайного числа заданной длины (в битах) посредством паттерна “фабричный метод”.

   Продемонстрируйте выполнение реализованного функционала.

Задания к работе №4 по фундаментальным алгоритмам.

1. Расширьте класс, реализованный во вспомогательном задании 1, следующим функционалом:
   - умножение чисел (алгоритмом Карацубы);
   - умножение чисел (на основе быстрого преобразования Фурье);
   - деление чисел (методом Ньютона);
   - быстрое возведение в степень;
   - быстрое возведение в степень по модулю;
   - алгоритм Евклида (в виде дружественной функции);
   - расширенный алгоритм Евклида (в виде дружественной функции);
   - бинарный алгоритм Евклида (в виде дружественной функции).

   Продемонстрируйте выполнение реализованного функционала.

2. Расширьте класс, реализованный в задании 1, следующим функционалом (в виде дружественных функций):
    - вычисление символа Лежандра;
    - вычисление символа Якоби;
    - определение простоты числа при помощи теста Ферма;
    - определение простоты числа при помощи теста Соловея-Штрассена;
    - определение простоты числа при помощи теста Миллера-Рабина.

    Продемонстрируйте выполнение реализованного функционала.

3. На базе класса из задания 2 реализуйте класс для алгоритма RSA, предоставляющий методы:
    - генерации ключей алгоритма, с параметризацией: длины чисел p и q (в битах), теста простоты (при помощи enum), значения минимальной вероятности простоты в диапазоне [0.5, 1);
    - выполнение шифрования при помощи сгенерированных ключей;
    - выполнение дешифрования при помощи сгенерированных ключей.

    Продемонстрируйте выполнение реализованного функционала. Докажите корректность алгоритма RSA.