Задание: Алгоритм Миллера-Рабина

Дедлайн – 3 недели

Перед тем, как прислать решение, обязательно прочтите требования к решениям

0. Изучить математические основы алгоритма Миллера-Рабина!
1. Реализовать тест простоты Миллера-Рабина для длинных чисел.
   a. Использовать реализованную ранее функцию для быстрого возведения в степень длинных чисел по модулю. Если она не написана, тогда нужно реализовать её самостоятельно, то есть нельзя использовать готовые библиотечные функции для возведения в степень.
   b. Написать функцию, которая проверяет длинное число p (p – **произвольное** положительное целое число) на простоту с помощью теста Миллера-Рабина. Эта функция должна принимать количество раундов n в виде параметра, по умолчанию количество раундов берется $n = \log p$, то есть, **по сути**, должна быть следующая функция:

```
def is_prime(p, n=log p):
    тело функции
is_prime(111) # количество раундов: log 1111
is_prime(111, 5) # количество раундов: 5
```

   c. Написать функцию, которая генерирует (возможно) простое число определенной битности. Например,

```
def generate_prime(n): // n - количество бит
    тело функции
generate_prime(3) # 7f
```

   d. Разработать консольное приложение, использующее описанную выше функцию для проверки на простоту числа/чисел, введенных пользователем в консоли, считанных из файла.
      - После запуска программы пользователю отображается «Главное меню» с тремя вариантами выбора: «Ввод с консоли», «Ввод из файла».
        - После выбора «Ввод с консоли»: пользователь вводит сначала число, которое нужно проверить на простоту, затем если пользователь захочет, у него должна быть возможность ввести количество раундов. Если пользователь не вводит количество раундов, тогда выбираем количество раундов как $n = \log p$. После этого запускается функция проверки на простоту, а результат

(составное или возможно простое) выводится на экран. В конце переходим к главному меню.

- После выбора «Ввод из файла»: пользователь вводит название файла. Файл состоит из некоторого количества строк. В каждой строке либо записано одно число p, либо два числа p и n. Например,

```
3
123 2
12345 4
```

Программа должна проверить каждое p на простоту с количество раундов n (если в строке n нет, тогда $n = \log p$). Результат (составное или возможно простое) должен выводиться в файл (либо попросите пользователя ввести название этого файла, либо выведите название файла пользователю, чтобы он знал, где искать) в следующем формате: число результат, например,

```
3 - возможно простое
123 2 - составное
12345 4 - составное
```

В конце переходим к главному меню.

Можно реализовать графическое приложение с эквивалентной функциональностью.

Допустимы незначительные изменения в интерфейсе (что выводится на экран, что вводит пользователь) с сохранением всех описанных выше функциональностей.