ОТЧЕТ

ЛАБОРАТОРНАЯ РАБОТА 1

ВАРИАНТ 8

Кражевский Алексей Игоревич, 15 группа

Результат выполнения программы:

```
Enter bit size:4
Generated number =  13
Test results:
        Miller-Rabin test:  True
        Fermet test:  True
Enter pow of mersen number (prime):13
Mersen number =  8191
        Luke-Lemer test for mersen number:  True
```

Тест Ферма:

По Теореме Ферма, если n – простое число, тогда для любого a справедливо следующее равенство $a^{n-1}=1 \pmod n$. Отсюда мы можем вывести правило теста Ферма на проверку простоты числа: возьмем случайное $a \in \{1, ..., n-1\}$ и проверим будет ли соблюдаться равенство $a^{n-1}=1 \pmod n$. Если равенство не соблюдается, значит скорее всего n – составное.

Оптимальное количество повторений – 20 (исходя из формулы определения вероятности).

Тест Миллера-Рабина:

Ввод: $n > 2$, нечётное натуральное число, которое необходимо проверить на простоту;
k – количество раундов.
Вывод: *составное*, означает, что n является составным числом;
вероятно простое, означает, что n с высокой вероятностью является простым числом.
Представить $n - 1$ в виде $2^s \cdot t$, где t нечётно. Это можно сделать последовательным делением $n - 1$ на 2.
цикл A: повторить k раз:
  Выбрать случайное целое число a в отрезке $[2, n - 2]$
  $x \leftarrow a^t \bmod n$, вычисляется с помощью возведения в степень по модулю
  если $x = 1$ или $x = n - 1$, то перейти на следующую итерацию цикла A
  цикл B: повторить $s - 1$ раз
    $x \leftarrow x^2 \bmod n$
    если $x = 1$, то вернуть *составное*
    если $x = n - 1$, то перейти на следующую итерацию цикла A
  вернуть *составное*
вернуть *вероятно простое*

Псевдокод Люка-Лемера:

```
LLT(p)
    ►Вход: простое нечётное число p
    S = 4
    k = 1
    M = 2^p – 1
    До тех пока k != p - 1 выполнять
        S = ((S × S) – 2) mod M
        k += 1
    Конец цикла
    Если S = 0 выполнять
        Возвратить ПРОСТОЕ
    иначе
        Возвратить СОСТАВНОЕ
    Конец условия
```

Мой код на вход принимает заранее сгенерированное число Мерсена и его степень и прогоняет тест для этого числа (результат на скриншоте).