Ермолаева Екатерина Александровна, 14 группа, лабораторная №1, 2 вариант

b) Тест Миллера-Рабина:

Алгоритм:

Вход: $n = 2^s r + 1$, r — нечетное.

Выход: 1 (n — простое) или 0 (n — простое?).

Шаги:

1. $a \xleftarrow{R} \{1, 2, 3, \ldots, n-1\}$.
2. Если $(a, n) \neq 1$, то возвратить 0.
3. $v \leftarrow a^r \bmod n$.
4. Если $v \equiv 1 \pmod{n}$, то возвратить 1.
5. Для $i = 0, \ldots, s-1$:
   (1) если $v \equiv -1 \pmod{n}$, то возвратить 1;
   (2) $v \leftarrow v^2 \bmod n$.
6. Возвратить 0.

Число запусков - 10 (так как вероятность ошибки при k запусках не превосходит 4^{-k}).

Полученное простое число - 1246884297130803558983006113151.

c) Тест Соловея-Штрассена:

Алгоритм:

Вход: $n > 2$, тестируемое нечётное натуральное число;
k, параметр, определяющий точность теста.

Выход: *составное*, означает, что n точно составное;
вероятно простое, означает, что n вероятно является простым.

for $i = 1, 2, \ldots, k$:
  a = случайное целое от 2 до $n-1$, включительно;
  если НОД(a, n) > 1, **тогда**:
    вывести, что n – составное, и **остановиться**.
  если $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$, **тогда**:
    вывести, что n – *составное*, и **остановиться**.

иначе вывести, что n – *простое с вероятностью* $1 - 2^{-k}$, и **остановиться**.

Число запусков - 20 (так как вероятность ошибки при k запусках не превосходит 2^{-k}).
Полученное простое число - 1047368171364062807551347517541.

c) Тест Люка-Лемера:
Алгоритм:

```
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
```

Число запусков - 1.
Полученное простое число - 2305843009213693951.