Вероятностные алгоритмы проверки чисел на простоту

Милёхин Александр НПМмд-02-21

Цель лабораторной работы

Изучение алгоритмов Ферма, Соловэя-Штрассена, Миллера-Рабина.

Критерии простоты

Для построения многих систем защиты информации требуются простые числа большой разрядности. В связи с этим актуальной является задача тестирования на простоту натуральных чисел.

Тест Ферма

- Вход. Нечетное целое число $n \geq 5$.
- Выход. «Число n, вероятно, простое» или «Число n составное».

1. Выбрать случайное целое число $a, 2 \leq a \leq n-2$.
2. Вычислить $r = a^{n-1}(mod n)$
3. При $r = 1$ результат: «Число n, вероятно, простое». В противном случае результат: «Число n составное»..

Тест Соловэя-Штрассена

- Вход. Нечетное целое число $n \geq 5$.
- Выход. «Число n, вероятно, простое» или «Число n составное».

1. Выбрать случайное целое число $a, 2 \leq a \leq n-2$.
2. Вычислить $r = a^{(\frac{n-1}{2})}(modn)$
3. При $r \neq 1$ и $r \neq n-1$ результат: «Число n составное».
4. Вычислить символ Якоби $s = (\frac{a}{n})$
5. При $r = s(modn)$ результат: «Число n, вероятно, простое». В противном случае результат: «Число n составное».

Тест Миллера-Рабина

1. Представить $n-1$ в виде $n-1=2^s r$, где r - нечетное число
2. Выбрать случайное целое число $a, 2 \leq a \leq n-2$.
3. Вычислить $y = a^r (mod n)$
4. При $y \neq 1$ и $y \neq n-1$ выполнить действия
   - Положить $j = 1$
   - Если $j \leq s-1$ и $y \neq n-1$ то
     - Положить $y = y^2 (mod n)$
     - При $y = 1$ результат: «Число n составное».
     - Положить $j = j+1$
   - При $y \neq n-1$ результат: «Число n составное».
5. Результат: «Число n, вероятно, простое».

Пример работы алгоритма

```
main()
```

```
Введите число для теста Ферма: 5
Тест Ферма для числа:  5
Число n, вероятно, простое
Тест Миллера-Рабина
Введите число для теста Миллера-Рабина: 5
Число n, вероятно, простое
Введите число для теста Соловэя-Штрассена: 5
5 Число n, вероятно, простое
```

Figure 1: Пример работы алгоритмов

Результаты выполнения лабораторной работы

Я изучил алгоритмы Ферма, Соловэя-Штрассена, Миллера-Рабина, а также реализовал данные алгоритмы программно на языке Python.

Спасибо за внимание