Вероятностные алгоритмы проверки чисел на простоту

Баранов Иван НФИмд 01-22 10

ноября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

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

Выполнение лабораторной работы

Наибольший общий делитель

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 $r = a^{n-1} \pmod{n}$
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 $r = a^{\left(\frac{n-1}{2}\right)} \pmod{n}$
3. При $r \neq 1$ и $r \neq n - 1$ результат: «Число n составное».
4. Вычислить символ Якоби $s = \left(\frac{a}{n}\right)$
5. При $r = s \pmod{n}$ 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, $2 \le a \le n-2$.
3. Вычислить $y = a^r \pmod n$
4. При $y \ne 1$ и $y \ne n-1$ выполнить действия
   - Положить $j = 1$
   - Если $j \le s-1$ и $y \ne n-1$ то
     - Положить $y = y^2 \pmod n$
     - При $y = 1$ результат: «Число n составное».
     - Положить $j = j+1$
   - При $y \ne n-1$ результат: «Число n составное».
5. Результат: «Число n, вероятно, простое».

Пример работы алгоритма

```
In [2]:  1 main()

Введите число для ферма15898
Тест ферма для числа  15898
Составное
Тест миллера рабина
Введите число для миллера рабина15898
простое!
не простое!
Введите число для соловея штрассена15898
15898 составное число
```

Figure 1: Работа алгоритма

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы Ферма, Соловэя-Штрассена, Миллера-Рабина.