Вероятностные алгоритмы проверки чисел на простоту

Тагиев Б. А.

09 ноября 2024

Российский университет дружбы народов, Москва, Россия

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

Тест Миллера-Рабина.

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

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».

Тест Ферма

```
n = 101
print(Ferma(n, 25))
print("==========")
print(Ferma(n+1, 25))
```

```
Simple
True
==========
Complex
False
```

Тест Соловэя-Штрассена

```
print(SoloveiStrassen(n, 25))
print("==========")
print(SoloveiStrassen(n+1, 25))
```

```
True
==========
Complex
False
```

Тест Миллера-Рабина.

```
print(MillerRabin(n))
print("==========")
print(MillerRabin(n+1))
```

Тест Миллера-Рабина.

```
Complex
Complex
Complex
Complex
Complex
Complex
Complex
Complex
Simple
True
==========
Simple
Complex
False
```

Выводы

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