

Цели и задачи

Цель лабораторной работы

Изучение Вероятностные алгоритмы проверки чисел на простоту : алгоритмов Ферма , вычисления символа якоби, Соловья-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».

Алгоритм вычисления символа якоби

1. Если НОД $(a, b) \neq 1$, выход из алгоритма с ответом 0.
2. Инициализация. $r=1$
3. Переход к положительным числам. Если $a < 0$, то $a = -a$. Если $b \bmod 4 = 3$, то $r = -r$
4. Избавление от чётности. $t=0$. Цикл ПОКА a — чётное, $t=t+1$, $a=a/2$. Конец цикла. Если t — нечётное, то Если $b \bmod 8 = 3$ или 5, то $r = -r$.
5. Вычисление символа Якоби. 14 При перестановке аргументов больший заменяется на остаток от деления на меньший. Это возможно благодаря периодичности символа Якоби. Сложность алгоритма равна $O(\log a \cdot \log b)$ битовых операций.

Тест Соловья-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 $r = a^{\frac{n-1}{2}} \pmod n$
 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 $s \equiv r \pmod{n}$ 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 , $2 \leq a \leq n-2$.
3. Вычислить $y = a^r \pmod{n}$
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 $y = y^2 \pmod{n}$
 - 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

```
[58]: n = 2085
```

```
[59]: Fermat(n, 30)
```

Число Составное

```
[59]: False
```

```
[60]: calculateJacobian(30, n)
```

```
[60]: 0
```

```
[61]: SoloveiStrassen(n, 30)
```

Число Составное

```
[61]: False
```

```
[62]: MillerRabin(n)
```

Простое

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы Ферма, вычисления символа якоби, Соловья-Штрассена, Миллера-Рабина.