Цели и задачи

Цель лабораторной работы

зучение Вероятностные алгоритмы проверки чисел на простоту : алгоритов Ферма , вычисления символа якоби, 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 $r=a^{n-1} (mod n)$
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)≠1, выход из алгоритма с ответом 0.
2. Инициализация. r=1
3. Переход к положительным числам. Если a<0, то a=-a. Если b mod 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 mod 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 · log b) битовых операций.

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.

1. Представить $n-1$ в виде $n-1 = 2^sr$, 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

```
n = 31  # Простое число

print("Тест Ферма:")
fermat_test(n, 50)

print("Тест Соловея-Штрассена:")
solovay_strassen(n, 50)

print("Тест Миллера-Рабина:")
miller_rabin(n, 50)
```

```
Тест Ферма:
Вероятно, Простое
Тест Соловея-Штрассена:
Вероятно, Простое
Тест Миллера-Рабина:
Вероятно, Простое

True
```

{ #fig:001 }

Выводы

Результаты выполнения лабораторной работы

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