

Вероятностные алгоритмы проверки чисел на простоту.

Меньшов Иван Сергеевич

07 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучить вероятностные алгоритмы проверки чисел на простоту.

Выполнение лабораторной работы

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. Если $r = 1$ результат : “Число n , вероятно, простое”. В противном случае результат: “Число n составное”.

Вход. Нечетное целое число $n \geq 3$, целое число $a, 0 \leq a < n$.

Выход. Символ Якоби.

1. $g=1$
2. если $a=0$ результат: 0
3. если $a=1$ результат: g
4. представить a в виде $a = 2^k a_1$, где a_1 нечетное.
5. при четном k положить $s=1$, при нечетном положить $s=1$,
если $n \equiv 1 \pmod{8}$; положить $s=-1$, если $n \equiv 3 \pmod{8}$

6. при a_1 результат: gs
7. если $n = 3(\bmod 4)$ and $a_1 = 3(\bmod 4)$, то $s = -s$
8. положить $a = n \bmod(a_1)$ $n = a_1$ $g = gs$ и вернуться на шаг 2

Алгоритм , реализующий тест Соловея - 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 $r = a^{(n+1)/2} \pmod n$
3. Если r не равен 1 и $n-1$ результат: “Число n составное”.
4. Вычислить символ Якоби $s = (a/n)$
5. Если $r = s \pmod n$ результат: “Число n составное”, иначе “Число n , вероятно, простое”.

Алгоритм , реализующий 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
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 следующее
 - 4.1. положить $j = 1$

Алгоритм , реализующий тест Миллера - Рабина

4.2. если $j \leq s-1$ и y не равен $n-1$,то

4.2.1. положить $y = y^2 \pmod n$

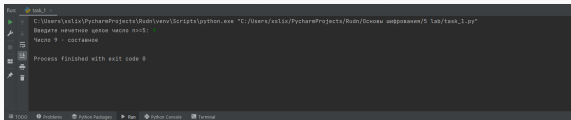
4.2.2. при $y = 1$ результат: "Число n составное"

4.2.3. положить $j = j+1$

4.3. при y не равном $n-1$ результат: "Число n составное"


5. Результат: "Число n , вероятно, простое"

Контрольные примеры



```
Run task_1.py
C:\Users\slis\PycharmProjects\Ruhr\venv\Scripts\python.exe "C:/Users/slisk/PycharmProjects/Ruhr/Scenarij informacion/5 lab/task_1.py"
Введите натуральное число n=5:
Число 9 - составное
Process finished with exit code 0
```

Figure 1: Тест Ферма



```
Run task_2.py
C:\Users\slis\PycharmProjects\Ruhr\venv\Scripts\python.exe "C:/Users/slisk/PycharmProjects/Ruhr/Scenarij informacion/5 lab/task_2.py"
Enter an odd number n=3:
Enter an integer 0<= a <= n:
-1
Process finished with exit code 0
```

Figure 2: Символ Якоби

Контрольные примеры



```
Run task_3
C:\Users\xsli\PycharmProjects\Radn\venv\Scripts\python.exe "C:/Users/xsli/PycharmProjects/Radn/venv/Scripts/task_3.py"
Введите нечетное число n=5:
Число 7, простое, простое
Process finished with exit code 0
```

Figure 3: Алгоритм , реализующий тест Соловея - Штрассена



```
Run task_4
C:\Users\xsli\PycharmProjects\Radn\venv\Scripts\python.exe "C:/Users/xsli/PycharmProjects/Radn/venv/Scripts/task_4.py"
Введите нечетное число n=5:
Число 7, простое, простое
Process finished with exit code 0
```

Figure 4: Алгоритм , реализующий тест Миллера - Рабина

Выводы

Мной были изучены вероятностные алгоритмы проверки чисел на простоту.