Отчёт по лабораторной работе №5

Дисциплина: Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна, НПМмд-02-23

Содержание

# 1 Цель работы

Изучить вероятностные алгоритмы проверки чисел на простоту.

# 2 Задание

Реализовать четыре теста на определение простоты чисел:

1. Тест Ферма
2. Символ Якоби
3. Тест Соловэя-Штрассена
4. Тест Миллера-Рабина

# 3 Теоретическое введение

Пусть а - целое число. Числа называются тривиальными делителями числа а.

Целое число называется простым, если оно не является делителем единицы и не имеет других делителей, кроме тривиальных. В противном случае число называется составным. Например, числа являются простыми.

Пусть . Целые числа а и вназываются сравнимыми по модулю m (обозначается ) если разность делится на m. Также эта процедура называется нахождением остатка от целочисленного деления а на b.

Проверка чисел на простоту является составной частью алгоритмов генерации простых чисел, применяемых в криптографии с открытым ключом. Алгоритмы проверки на простоту можно разделить на вероятностные и детерминированные.

*Детерминированный* алгоритм всегда действует по одной и той же схеме и гарантированно решает поставленную задачу (или не дает никакого ответа). *Вероятностный* алгоритм использует генератор случайных чисел и гарантированно точный ответ. Вероятностные алгоритмы в общем случае не менее эффективны, чем детерминированные (если используемый генератор случайных чисел всегда дает набор одних и тех же чисел, зависящих от входных данных, то вероятностный алгоритм становится детерминированным).

Для проверки на простоту числа n вероятностным алгоритмом выбирают случайной число а и проверяют условия алгоритма. Если число n не проходит тест по основанию а, то алгоритм выдает результат «Число п составное», и число п действительно является составным.

Если же n проходит тест по основанию а, ничего нельзя сказать о том, действительно ли число n является простым. Последовательно проведя ряд проверок таким тестом для разных а и получив для каждого из них ответ «Число n, вероятно, простое», можно утверждать, что число n является простым с вероятностью, близкой к 1. После с независимых выполнений теста вероятность того, что составное число и будет t раз объявлено простым (вероятность ошибки), не превосходит .

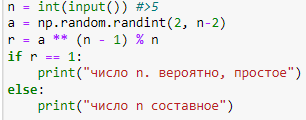
*Тест Ферма* основан на малой теореме Ферма: для простого числа р и произвольного числа а, , выполняется сравнение

Следовательно, если для нечетного n существует такое целое а, что , НОД(а, n) = 1 и , то число п составное.

Более подробно см. в [1–6].

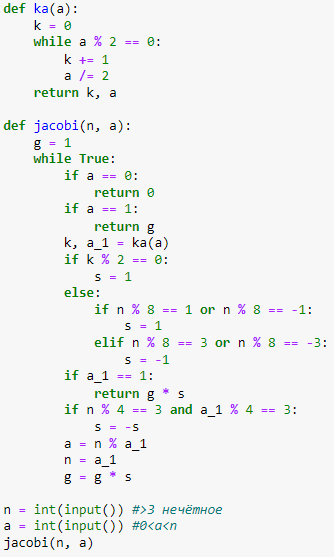
# 4 Выполнение лабораторной работы

1. Реализуем тест Ферма (рис. ??).



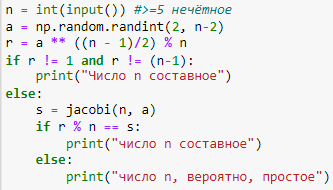
Тест Ферма

1. Реализуем алгоритм нахождения символа Якоби (рис. ??).



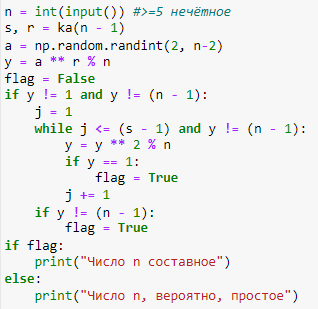
Символ Якоби

1. Реализуем тест Соловэя-Штрассена (рис. ??).



Тест Соловэя-Штрассена

1. Реализуем тест Миллера-Рабина (рис. ??).



Тест Миллера-Рабина

# 5 Выводы

Изучила вероятностные алгоритмы проверки чисел на простоту.

# Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.

2. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Robbins A. [Bash Pocket Reference](https://www.ncbi.nlm.nih.gov/pubmed/25246403). O’Reilly Media, 2016. 156 с.

5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.

6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.