* Тест Міллера – Рабіна

Цей алгоритм параметрізуется кількістю раундів *r*.

Для даного *n* знаходиться таке ціле число *s* і ціле непарне число *t*, що

|  |
| --- |
|  |

Вибирається випадкове число *a*, 1 < *a* < *n*. Якщо *a* не є свідком простоти числа *n*, то видається відповідь «*n* - складене», і алгоритм завершується. Інакше, вибирається нове випадкове число *a*, і процедура перевірки повторюється. Після знаходження *r* свідків простоти видається відповідь «*n* - ймовірно просте», і алгоритм завершується.

Алгоритм Гордона дозволяє генерувати «сильне» просте число. Під час його реалізації повинен бути використаний імовірнісний або детермінований тест перевірки на простоту. У нашому випадку був використаний імовірнісний тест – Тест Міллера – Рабіна.

Алгоритм Міллера – Рабіна починається з перевірки числа на окремі випадки: якщо число = 2, або = 3, тоді воно просте; якщо число = 1, або воно парне, тоді це число складене. Потім нам потрібно наше число представити у вигляді *.* Після цього робимо цикл А, який повторюємо разів. Рекомендується брати *k* порядку величини

|  |  |
| --- | --- |
|  |  |

де *n* - перевіряєме число.

У циклі вибираємо випадкове число з проміжку [2, *n -*2]. Виконуємо операцію піднесення до степеня за модулем числа

|  |
| --- |
|  |

Якщо *x* = 1 або *x = n –* 1, то наше число складене. Потім у циклі А робимо внутрішній цикл В, який повторюємо *s* – 1 разів. У ньому виконуємо дію

|  |
| --- |
| . |

Якщо *x =* 1 або *x = n* - 1 то число складене. На цьому операції у циклах закінчуються, якщо число пройшло всі операції то вона імовірносне просте.

Загальній алгоритм роботи програми зображено на рисунку 1.3. При запуску програми відбувається генерація двох простих чисел та перевірка їх на простоту за тестом Міллера – Рабіна. Якщо ці числа не прості, тобто складені, тоді ми знову генеруємо їх, поки вони не будуть простими. Після того як сгенерувалися псевдопрості числа, ми вибираємо ціле число *і.* У нашому випадку *і =* 3. Потім у послідовності шукаємо перше просте число через перевірку на простоту тестом Міллера – Рабіна. Позначаємо це число *r.* Після цього за допомогою функції піднесення числа до степеня по модулю числа обраховуємо

|  |
| --- |
|  |

підставляємо це значення у вираз

|  |  |
| --- | --- |
|  |  |

Знову вибираємо ціле число *j.* У нашому випадку *j =* 5. У послідовності шукаємо перше просте число через перевірку на простоту тестом Міллера – Рабіна. Позначаємо це число *p,* яке і є «сильним». На цьому етапі розрахунок «сильного» простого числа завершено. На екрані зявляється запис: Сгенеровано сильне просте число *p*. Для генерації нового «сильного» простого числа користувачу програми потрібно закрити та знову її запустити.