Лабораторная работа №5

Вероятностные тесты на простоту чисел

Выполнил: Хамза Хуссен

Цель работы:

Изучение, программная реализация и сравнительный анализ трёх вероятностных алгоритмов проверки чисел на простоту:

Тест Ферма

Тест Соловэя-Штрассена

Тест Миллера-Рабина

Практическая значимость: Эти алгоритмы являются фундаментом для генерации больших простых чисел, используемых в современных криптографических системах (RSA, цифровые подписи).

Классификация тестов на простоту

Два подхода к проверке простоты:

Детерминированные тесты

✅ Дают строгое доказательство простоты.

❌ Вычислительно сложны для больших чисел.

❌ Чаще используются для целенаправленной генерации.

Вероятностные тесты

✅ Высокая скорость для больших чисел.

✅ Вероятность ошибки может быть сделана сколь угодно малой.

✅ Широко применяются для первичной

Золотой стандарт на практике: Комбинация быстрого вероятностного теста (Миллера-Рабина) с последующим детерминированным тестом для подтверждения.

Обобщение теста Ферма с использованием символа Якоби.

Алгоритм (ключевые шаги):
Выбрать случайное основание a.

Вычислить r = a^((n-1)/2) mod n.

Вычислить символ Якоби s = (a/n).

Проверить условие: r ≡ s (mod n).

Если условие выполняется → число вероятно простое.

Особенность: Более надёжен, чем тест Ферма, но требует вычисления символа Якоби, что несколько замедляет работу.

Бинарный алгоритм Евклида

Идея: Оптимизация за счёт использования битовых операций (деление/умножение на 2).
Основные шаги:

Факторизация двойки: Пока a и b чётные, делим их на 2 и запоминаем множитель g.

Основной цикл:

Делим u и v на 2, пока они чётные.

Вычитаем меньшее из большего: u = u - v или v = v - u.

Повторяем, пока u != 0.

Результат: НОД = g * v.

Преимущество: Высокая скорость на компьютерах.

Более строгий анализ сравнений по модулю.

Подготовка:
Разложить n-1 в виде: $n-1 = 2^s * d$, где d — нечётное.

Алгоритм (основная логика):
Для случайного a вычислить последовательность:
a^d, a^{2d}, a^{4d}, ..., $a^{2^{s-1}d}$ (всё по модулю n).

Если первый элемент не равен 1, а в последовательности нет элемента n-1 → число составное.

Преимущество: Самый надёжный из трёх рассмотренных вероятностных тестов. Вероятность ошибки ≤ 4^{-k} (для k испытаний).

Сравнительный анализ алгоритмов

Критерий	Ферма	Соловэй-Штрассен	Миллер-Рабин
Скорость	Самый быстрый	Средняя	Высокая
Надёжность	Низкая (есть Кармайкла)	Высокая	Очень высокая (стандарт)
Сложность реализации	Простейшая	Средняя (символ Якоби)	Средняя
Применение на практике	Редко, как составная часть	Историческое значение	Основной вероятностный тест

Результаты выполнения (Контрольный пример)

Тестовые числа: [17, 25, 97, 100, 561] Вывод программы:

Введите первое число (a): 30
Введите второе число (b): 18

1. Простой алгоритм Евклида:
   НОД(30, 18) = 6
Тестируем число: 17
Ферма: Простое
Соловэй-Штрассен: Простое
Миллер-Рабин: Простое
Тестируем число: 25
Ферма: Составное
Соловэй-Штрассен: Составное
Миллер-Рабин: Составное

Тестируем число: 561 (Число Кармайкла)
Ферма: Простое <-- Ошибка!
Соловэй-Штрассен: Составное
Миллер-Рабин: Составное
2. Расширенный алгоритм Евклида:
   НОД(30, 18) = 6
   Коэффициенты: 30*(-1) + 18*(2) = 6
   # Проверка: 30*(-1) + 18*2 = -30 + 36 = 6

Вывод: Тесты Соловэя-Штрассена и Миллера-Рабина корректно определили число Кармайкла (561) как составное, а тест Ферма — ошибся.

Выводы

В результате работы:

Критерий	Ферма	Соловэй-Штрассен	Миллер-Рабин
Скорость	Самый быстрый	Средняя	Высокая
Надёжность	Низкая (есть Кармайкла)	Высокая	Очень высокая (стандарт)
Сложность реализации	Простейшая	Средняя (символ Якоби)	Средняя
Применение на практике	Редко, как составная часть	Историческое значение	**Основной вероятностный тест**

Выводы и заключение

Итоги работы:
Изучены теоретические основы и реализованы три классических вероятностных теста на простоту.

Тест Миллера-Рабина подтвердил статус наиболее надёжного и рекомендуемого к практическому применению.

Продемонстрирован ключевой недостаток теста Ферма – неспособность обнаруживать числа Кармайкла.

Тест Соловэя-Штрассена показал высокую надёжность, но уступает тесту Миллера-Рабина по эффективности.