Лабораторная работа №5

Wang Yao

RUDN University, Moscow, Russian Federation

3 января 2026

Цель работы

Изучить теоретические основы вероятностных алгоритмов проверки чисел на простоту, реализовать три теста (Ферма, Соловэя–Штрассена, Миллера–Рабина) и провести сравнительный анализ их эффективности и точности.

Ход лабораторной работы

Основные понятия

- **Простое число**: имеет ровно два делителя — 1 и само себя
- **Составное число**: имеет более двух делителей
- **Вероятностный алгоритм**: использует случайность, даёт ответ с некоторой вероятностью ошибки
- **Детерминированный алгоритм**: всегда выдаёт точный результат
- **Число Кармайкла**: составное число, которое ведёт себя как простое по малой теореме Ферма

Тест Ферма

Основа: Малая теорема Ферма

Если p — простое число и $1 \leq a < p$, то:

$$a^{p-1} \equiv 1 \pmod{p}$$

Алгоритм: 1. Выбрать случайное $a \in [2, n-2]$ 2. Вычислить $r = a^{n-1} \bmod n$ 3. Если $r \neq 1 \rightarrow n$ **составное**

Иначе $\rightarrow n$ **вероятно простое**

Недостаток: Не обнаруживает числа Кармайкла

Тест Соловэя–Штрассена

Основа: Критерий Эйлера + символ Якоби

Для нечётного простого числа p и целого a:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Алгоритм: 1. Выбрать случайное $a \in [2, n-2]$ 2. Вычислить $r = a^{(n-1)/2} \bmod n$ 3. Вычислить символ Якоби $s = \left(\frac{a}{n}\right)$ 4. Если $r \not\equiv s \pmod{n} \to n$ **составное**

Преимущество: Более надёжен, чем тест Ферма

Тест Миллера–Рабина

Основа: Разложение $n - 1 = 2^s \cdot d$, где d — нечётное

Алгоритм: 1. Записать $n - 1 = 2^s \cdot d$, где d — нечётное 2. Выбрать случайное $a \in [2, n - 2]$ 3. Вычислить $x = a^d \bmod n$ 4. Если $x = 1$ или $x = n - 1$ → проходит 5. Для $r = 0$ до $s - 1$: - $x = x^2 \bmod n$ - Если $x = n - 1$ → проходит - Если $x = 1$ → **составное** 6. Если ни разу не получили $n - 1$ → **составное**

Преимущество: Наиболее надёжен из вероятностных тестов

Результаты тестирования

Число	Тип	Тест Ферма	Соловэя–Штрассена	Миллера–Рабина
17	Простое	√	√	√
25	Составное	√	√	√
97	Простое	√	√	√
561	Кармайкл	×	√	√

Примечание: 561 = 3 × 11 × 17 — первое число Кармайкла

Сравнительный анализ тестов

Параметр	Тест Ферма	Соловэя–Штрассена	Миллера
Сложность	$O(\log^3 n)$	$O(\log^3 n)$	$O(\log^3 n$
Вероятность ошибки	Высокая	$1/2$ за итерацию	$1/4$ за и
Надёжность	Низкая	Средняя	Высокая
Обнаружение Кармайкла	Нет	Да	Да
Практическое применение	Ограничено	Редко	Широко
Память	$O(1)$	$O(1)$	$O(1)$

Криптографическое значение

• **Генерация ключей**: Вероятностные тесты используются для генерации больших простых чисел в RSA, DSA, Diffie-Hellman

• **Безопасность**: Тест Миллера–Рабина с достаточным количеством итераций обеспечивает вероятность ошибки менее 2^{-100}

• **Производительность**: Вероятностные тесты значительно быстрее детерминированных для больших чисел

Вывод

Изучили и реализовали три вероятностных теста проверки чисел на простоту: Ферма, Соловэя–Штрассена и Миллера–Рабина.

Основные выводы:

• **Теоретическая ценность**: Понимание математических основ вероятностной проверки простоты

• **Практическая значимость**: Эти алгоритмы критически важны для криптографических систем

• **Сравнительный анализ**: - Тест Ферма: прост, но ненадёжен из-за чисел Кармайкла - Тест Соловэя–Штрассена: более надёжен, но сложнее в реализации - Тест Миллера–Рабина: наиболее надёжен и широко используется на практике

• **Криптографическое применение**: Тест Миллера–Рабина является стандартом для генерации простых чисел в RSA и других криптосистемах

• **Итоговый вывод**: Вероятностные тесты обеспечивают эффективный баланс между точностью и производительностью, что делает их незаменимыми в современных криптографических приложениях.

Литература

1. Теория чисел и криптография. — М.: Физматлит, 2018.