Лабораторная работа №5

Вероятностные алгоритмы проверки чисел на простоту

Студент: Ван Яо
Группа: НФИмд-01-25
РУДН, 2025

Цель работы

1. Изучить теоретические основы вероятностных алгоритмов проверки чисел на простоту
2. Реализовать программно три теста:
   - Тест Ферма
   - Тест Соловэя–Штрассена
   - Тест Миллера–Рабина
3. Провести сравнительный анализ их **эффективности** и **точности**

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

Тест Ферма

Основа: Малая теорема Ферма

$$a^{p-1} \equiv 1 \pmod{p}, \quad \text{если } p \text{ — простое и } \gcd(a,p) = 1$$

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**

Тест Соловэя–Штрассена

Основа: Критерий Эйлера + символ Якоби

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

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

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

Тест Миллера–Рабина

Наиболее популярный на практике (используется в RSA, TLS и др.)

Алгоритм: 1. Записать $n - 1 = 2^s \cdot r$, где r — нечётное 2. Для случайного a вычислить $y = a^r \bmod n$ 3. Если $y = 1$ или $y = n - 1 \rightarrow$ проходит 4. Иначе возводим y в квадрат до $s - 1$ раз: - Если получаем $n - 1 \rightarrow$ проходит - Если получаем 1 до этого $\rightarrow$ **составное** 5. Если ни разу не получили $n - 1 \rightarrow$ **составное**

Пример реализации: Тест Ферма

Число	Тип	Тест Ферма	Миллер–Рабин	Комментарий
17	Простое	√	√	Корректно
25	Составное	√	√	Корректно
97	Простое	√	√	Корректно
561	Кармайкл	×	√	Ферма обманут!

*Число **561 = 3 × 11 × 17** — первое число Кармайкла.*

Выводы

- Все три алгоритма реализованы и протестированы
- **Тест Ферма ненадёжен** из-за чисел Кармайкла
- **Тест Миллера–Рабина** показал **наивысшую надёжность**
- Он эффективен, масштабируем и широко используется в реальных системах безопасности

Спасибо за внимание!