Лабораторная работа №5

Вероятностные алгоритмы проверки чисел на простоту

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Назарова Дарья Владиславовна

Цель лабораторной работы

Теория

Изучить математические основы вероятностных тестов простоты: Ферма, Соловэя-Штрассена и Миллера-Рабина

Практика

Реализовать алгоритмы на языке Julia с обработкой граничных случаев

Анализ

Провести тестирование и сравнение эффективности различных алгоритмов

Теоретическая основа

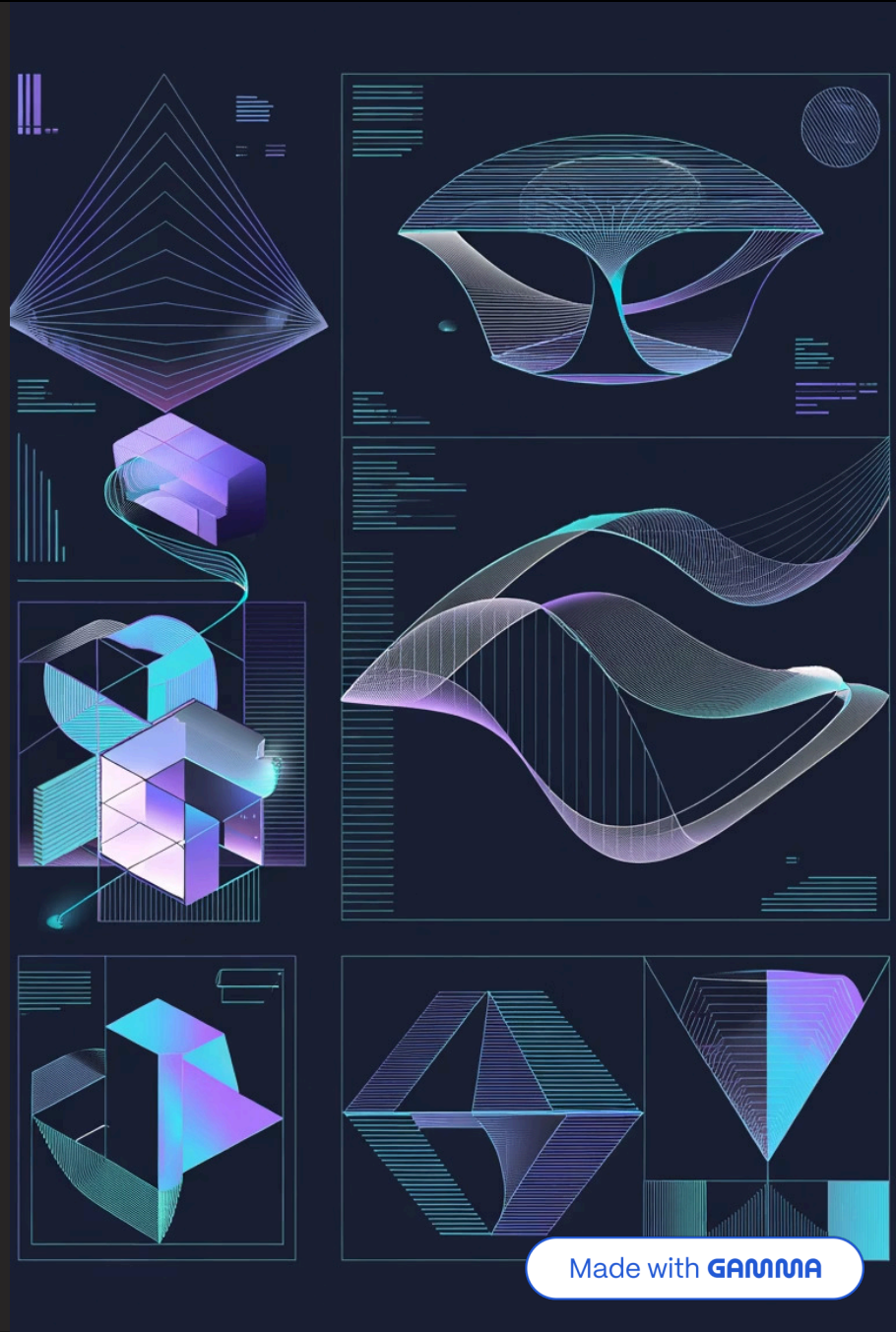
Простые числа

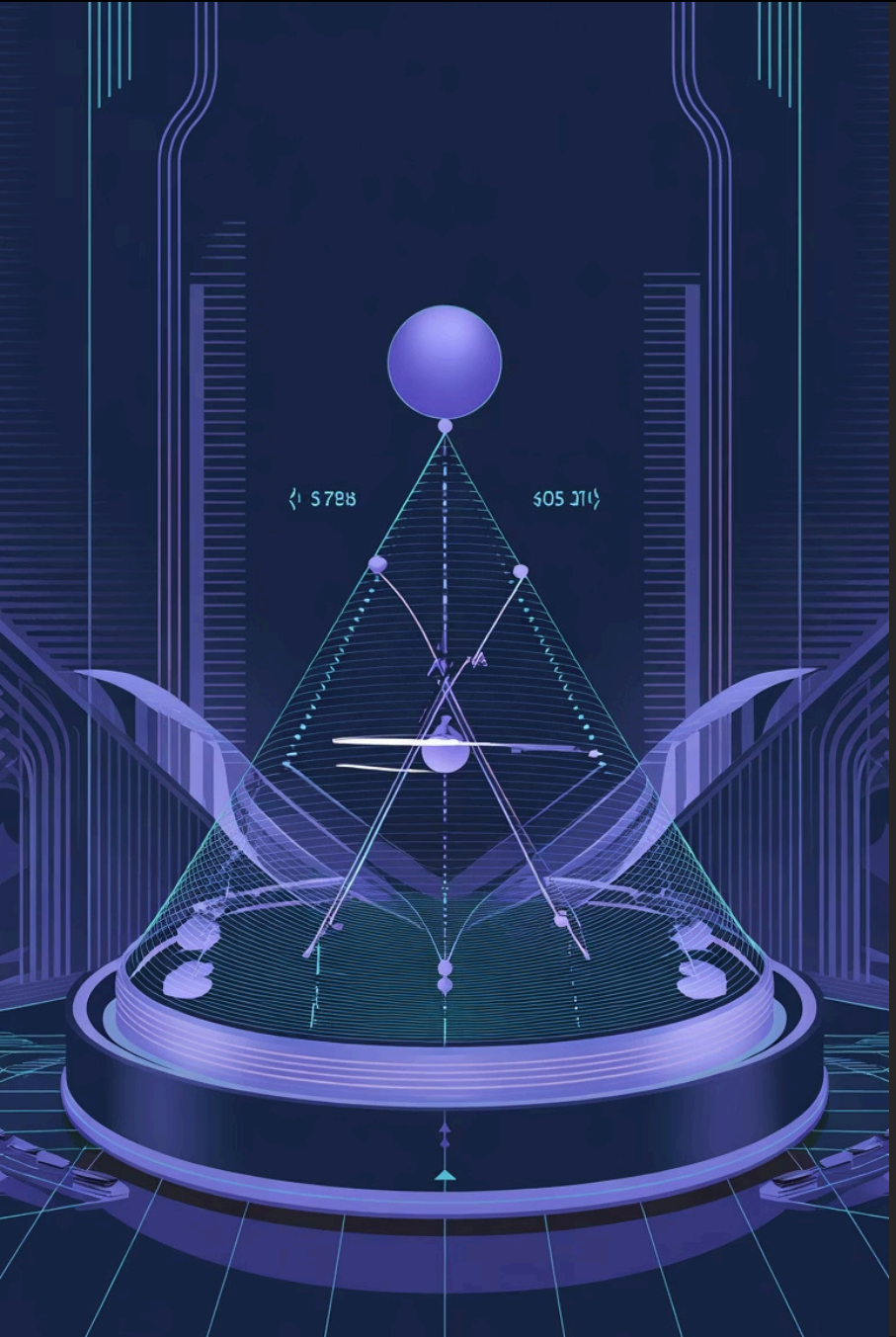
Натуральные числа, имеющие ровно два натуральных делителя: единица и само число. Фундаментальный объект теории чисел и криптографии.

Вероятностные алгоритмы

Алгоритмы, использующие генератор случайных чисел. Дают ответ с определённой вероятностью точности. Вероятность ошибки ≤ $1/2^t$ после t итераций.

Применение в криптографии: Широко используются в RSA и других системах защиты информации, где требуется быстрая проверка больших чисел на простоту.





Тест Ферма

Основа теста

Малая теорема Ферма: если p простое число и НОД(a,p)=1, то $a^{p-1} \equiv 1 \pmod{p}$

Алгоритм

1. Выбрать случайное a ∈ [2, n-2]
2. Вычислить $a^{n-1} \bmod n$
3. Если результат ≠ 1, число составное
4. Повторить k раз для увеличения надёжности

Преимущества

- Простота реализации
- Быстрое выполнение

Недостатки

- Числа Кармайкла
- Недостаточная надёжность

Символ Якоби

Обобщение символа Лежандра на составные модули. Критический инструмент для теста Соловэя-Штрассена и других тестов на простоту.

1 Определение

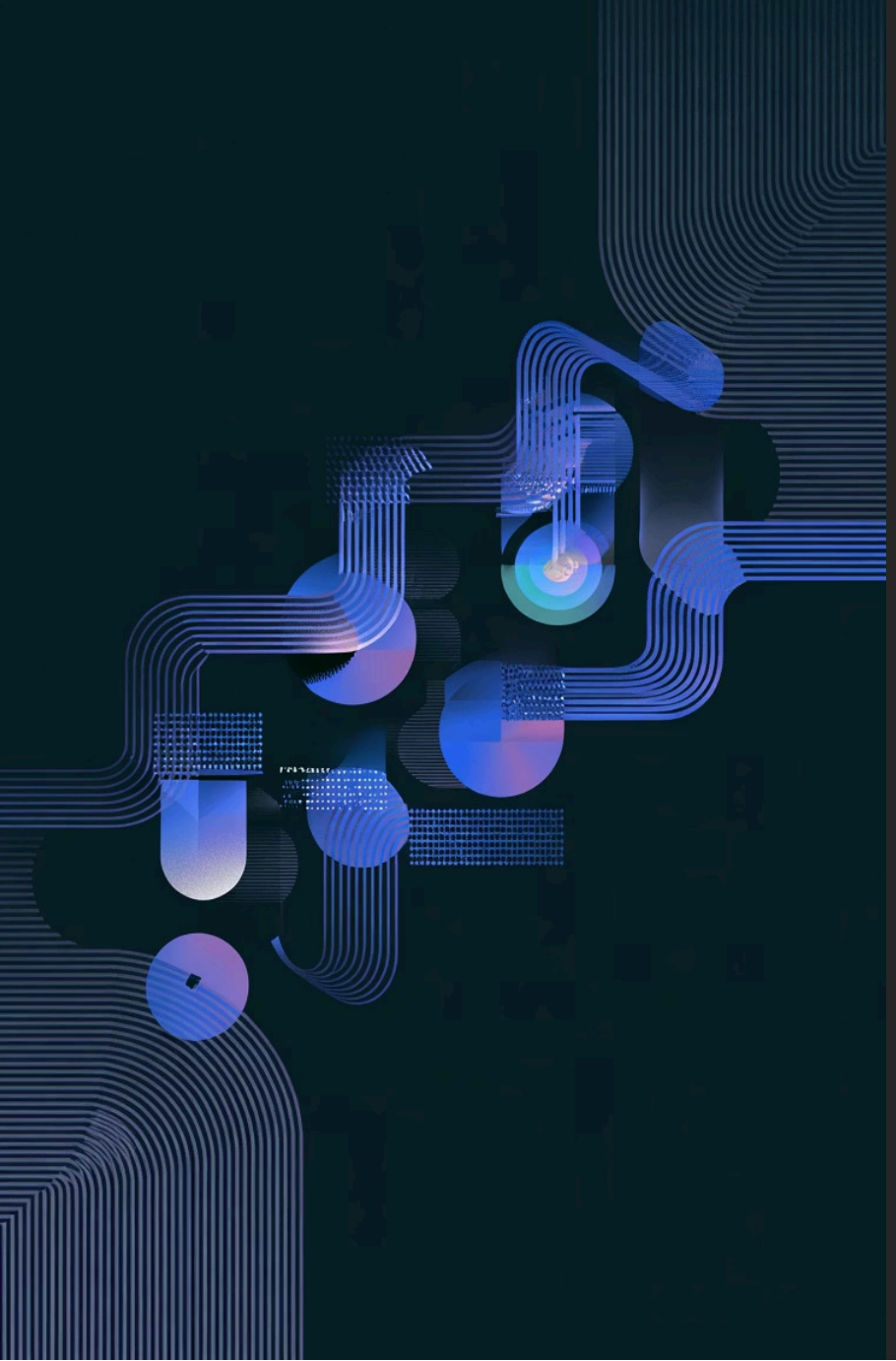
Мультипликативная функция, определённая для нечётных n и любых целых a

2 Ключевые свойства

(0/n) = 0; (1/n) = 1; (2/n) зависит от n mod 8; квадратичный закон взаимности

3 Вычисление

Рекурсивное вычисление с использованием факторизации по степеням 2 и нечётным множителям



Тест Соловэя-Штрассена

01

Критерий Эйлера

Для нечётного простого p: $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$

02

Выбор свидетеля

Выбрать случайное a и вычислить остаток $r = a^{(n-1)/2} \bmod n$

03

Вычисление символа

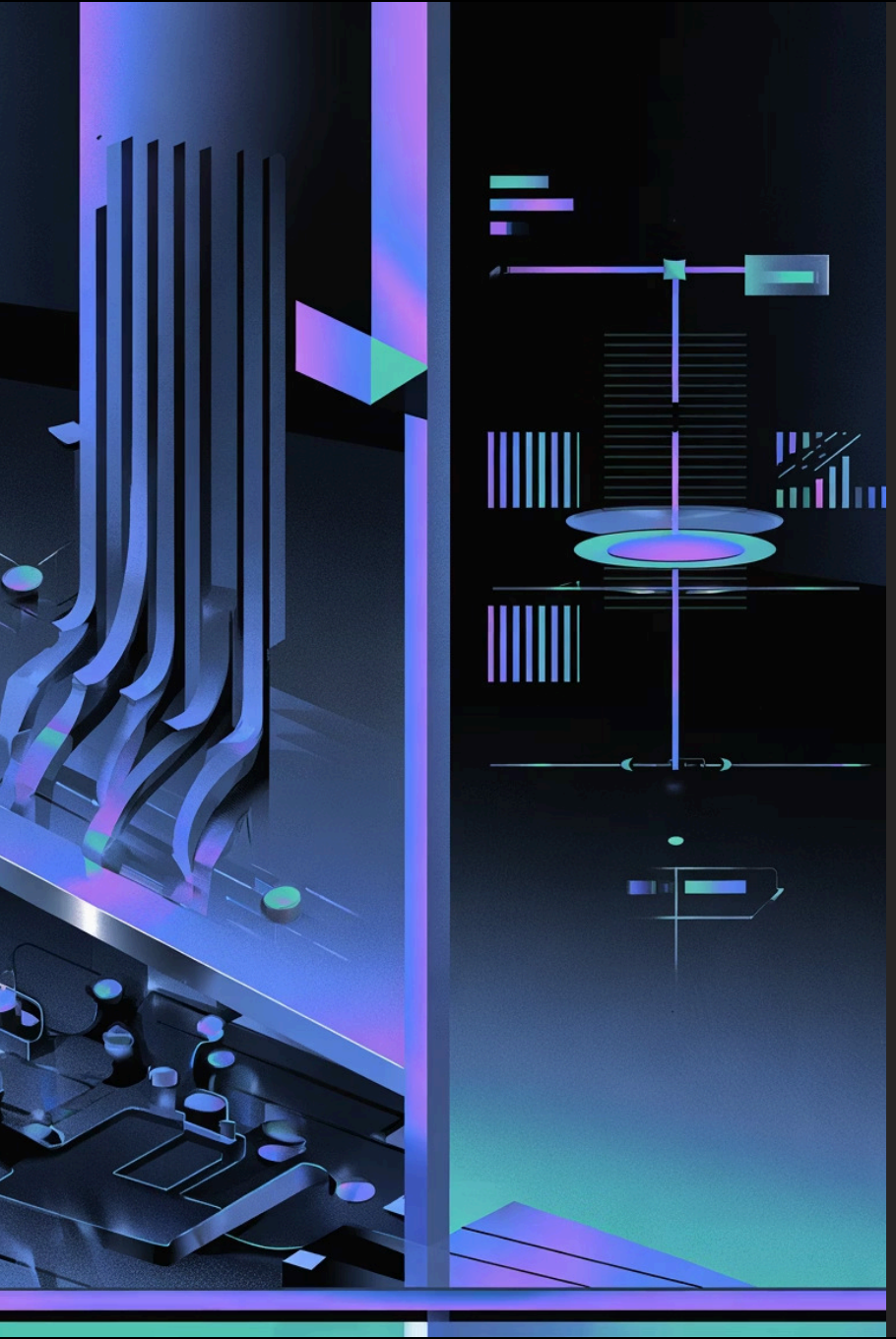
Найти символ Якоби s = (a/n) нормализованный к диапазону [0,n)

04

Проверка

Если $r \neq s \pmod{n}$, то число n составное; иначе, вероятно простое

Надёжность: Существенно выше, чем у теста Ферма. Вероятность ошибки ≤ 1/2 за одну итерацию.



Тест Миллера-Рабина

Наиболее надёжный вероятностный тест простоты, основанный на разложении $n-1 = 2^s \cdot r$.

Разложение

Представить n-1 в виде $2^s \cdot r$, где r нечётно

Выбор базиса

Выбрать случайное $a \in [2, n-2]$

Последовательность

Вычислить: a^r, a^{2r}, ..., $a^{2^{s-1}r}$ mod n

Вывод

Проверить условия простоты для последовательности

Преимущество: Вероятность ошибки ≤ 1/4 за одну итерацию. При 10 итерациях ≤ $1/2^{20}$.

Реализация на языке Julia

Ключевые компоненты

- Модульное возведение в степень (fast exponentiation)
- Рекурсивное вычисление символа Якоби
- Обработка граничных случаев (чётные числа, n ≤ 1)
- Параметризация количества итераций для управления вероятностью ошибки

Все три алгоритма реализованы с использованием встроенных функций Julia для модульной арифметики и побитовых операций.

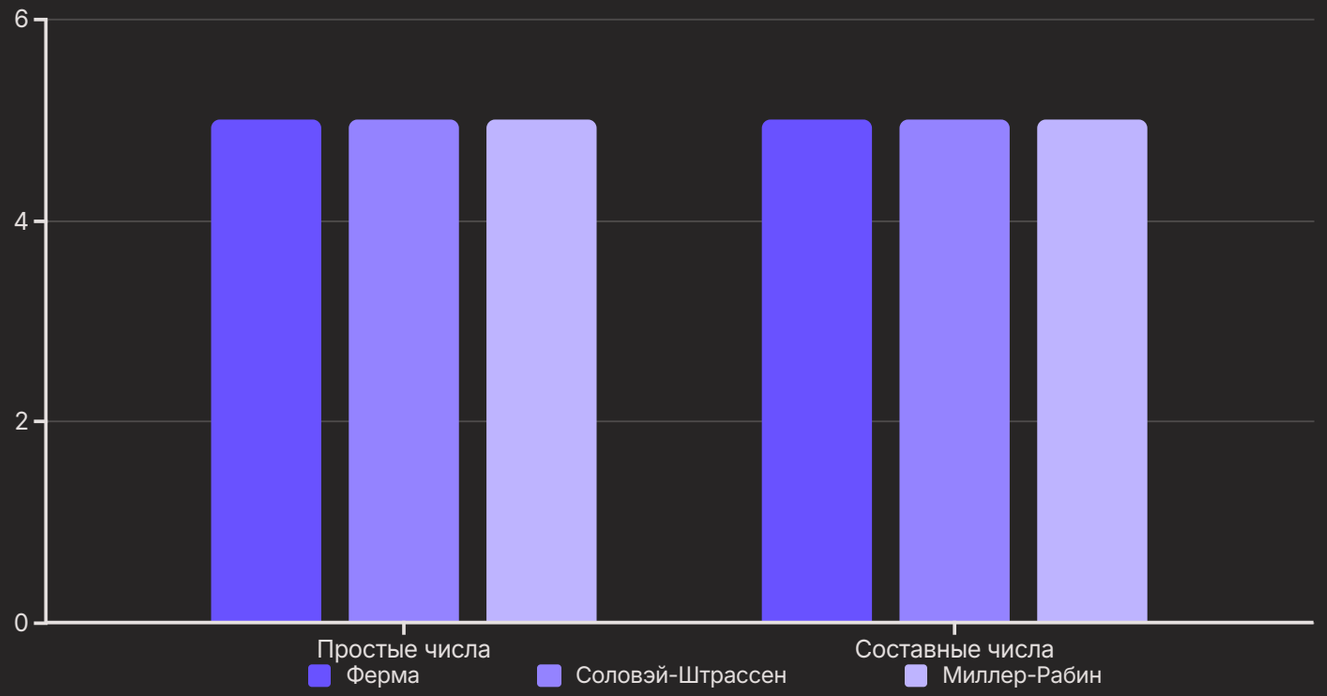
```
miller_rabin_test(101,
10)
# "Число 101,
вероятно,
# простое"

fermat_test(97, 5)
# "Число 97, вероятно,
# простое"

solovay_strassen_test(8
9, 8)
# "Число 89, вероятно,
# простое"
```

Результаты тестирования

Тестовые данные: 5, 9, 13, 15, 17, 21, 23, 29, 31, 33



100%

Точность Ферма

Корректно определены все числа

100%

Точность Соловэя-Штрассена

Корректно определены все числа

100%

Точность Миллера-Рабина

Наибольшая надёжность и корректность

Вероятность ошибки при 10 итерациях: ≤ 0.001 (1/1024). Все алгоритмы показали высокую надёжность при корректной реализации.

Выводы и рекомендации

1

Успешная реализация

Все три вероятностных алгоритма успешно реализованы на Julia с полной функциональностью и обработкой граничных случаев

2

Практическое применение

Тест Миллера-Рабина рекомендуется для криптографических приложений благодаря наивысшей надёжности и эффективности

3

Развитие

Возможны оптимизации для больших чисел, использование детерминированных вариантов и параллельные вычисления

Итоговая рекомендация: Вероятностные тесты простоты остаются незаменимым инструментом современной криптографии и теории чисел, обеспечивая баланс между скоростью и надёжностью проверки.