ЛАБОРАТОРНАЯ РАБОТА №5

Вероятностные алгоритмы проверки чисел на простоту

Кузнецов Юрий Владимирович

Введение

В данном отчёте будет представлена реализация вероятностных алгоритмов проверки чисел на простоту

Основное содержание

Шифры простой замены:

- Тест Ферма
- Символ Якоби
- Тест Соловэя-Штрассена
- Тест Миллера-Рабина

Кодовая реализация

Тест Ферма

```
function fermat_test(number)
  if number < 5
      return "Invalid."
  end
  base = rand(2:number-2)
  result = powermod(base, number-1, number)
  if result == 1
      return "$number`s simple."
  else
      return "$number`s composite."
  end
end

println(fermat_test(234))
```

Символ Якоби

```
ffunction jacobi_symbol(a, n)
  if n < 3 || a >= n || a < 0
      return "Invalid"
  end
  result = 1
  while a != 0
      count = 0
      while a % 2 == 0
          count += 1
          a ÷= 2
      end

      if count % 2 == 1 && (n % 8 == 3 || n % 8 == 5)
          result *= -1
      end

      if n % 4 == 3 && a % 4 == 3
          result *= -1
      end

      a, n = n % a, a
  end
  return n == 1 ? result : 0
end

println(jacobi_symbol(23, 32))
```

Тест Соловэя-Штрассена

```
function solovay_strassen(number)
  if number < 5
    return "Invalid"
  end

  base = rand(2:number-2)

  power = powermod(base, (number - 1) ÷ 2, number)
  if power != 1 && power != number - 1
    return "$number`s composite."
  end
  jacobi = jacobi_symbol(base, number)
  if power == jacobi
    return "$number`s composite."
  else
    return "$number`s probably prime."
  end

end

println(solovay_strassen(12345))
```

Тест Миллера-Рабина

```
function miller_rabin(number)
  if number < 5
```

```
        return "Invalid"
    end
    remainder = number - 1
    power = 0
    while remainder % 2 == 0
        power += 1
        remainder ÷= 2
    end
    base = rand(2:number-2)
    current = powermod(base, remainder, number)
    if current != 1 && current != number-1
        for _ in 1:power-1
            current = (current^2) % number
            if current == 1
                return "$number`s composite."
            end
        end
        if current != number-1
            return "$number`s composite."
        end
    end
    return "$number`s simple."
end

println(miller_rabin(12349))
```

Заключение

В данной лабораторной работе были реализованы вероятностные алгоритмоы проверки чисел на простоту