Лабораторная работа №6

Разложение чисел на множители

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

Цель работы

1. Изучить теоретические основы алгоритмов разложения чисел на множители
2. Реализовать программно два метода:
   - ρ-метод Полларда
   - Метод квадратов Ферма
3. Провести сравнительный анализ их **эффективности** и **точности**

Основные понятия

- **Факторизация**: разложение составного числа на простые множители
- **Нетривиальный делитель**: делитель, отличный от 1 и самого числа
- **ρ-метод**: вероятностный алгоритм, использующий поиск циклов
- **Метод Ферма**:основан на представлении числа как разности квадратов

ρ-метод Полларда

Основа: поиск цикла в последовательности $x_{i+1} = f(x_i)$
Особенности: 1. Использует “черепаху и зайца” для поиска цикла 2. Эффективен для чисел с малыми делителями 3. Сложность: $O(\sqrt{p})$ где p - наименьший делитель

```python
def pollards_rho(n,c=1,f=None,max_iterations=1000000):
    if n%2==0:
        return 2
    if f is None:
        f = lambda x:(x*x+1)%n

    a=c
    b=c

    for i in range(max_iterations):
        a=f(a)
        b=f(f(b))
        d=gcd(abs(a-b),n)

        if 1<d<n:
            return d
        if d==n:
            return None

    return None
```

Метод квадратов Ферма

Основа: $n = s^2 - t^2 = (s - t)(s + t)$

Алгоритм: 1. Эффективен когда делители близки к $\sqrt{n}$ 2. Прост в реализации 3. Медленный для чисел с сильно различающимися делителями

```python
def fermat_factorizaton(n,max_iterations=1000000):
    if n%2==0:
        return 2

    s=math.isqrt(n)
    if s*s==n:
        return s

    s+=1
    for i in range(max_iterations):
        t2=s*s-n
        t=math.isqrt(t2)

        if t*t==t2:
            p=s-t
            if p>1 and n%p==0:
                return p
            q=s+t
            if q<n and n%q==0:
                return q
            return p

        s+=1

        if s>(n+1)/2:
            break
    return None
```

Пример работы: ρ-метод

n	Функция	Делитель	Второй делитель
1359331	$x^2 + 5$	1181	1151
10403	$x^2 + 5$	103	101

Пример работы: Метод Ферма

n	Найденный s	t	Делители
1359331	1166	15	1151×1181
10403	102	1	101×103

Сравнительный анализ

Метод	Преимущества	Недостатки
ρ -метод Полларда	Быстрый на малых делителях	Может не сойтись для некоторых чисел
Метод квадратов Ферма	Простота реализации	Медленный, если делители далеки от $\sqrt{n}$

ρ-метод лучше для чисел с небольшими простыми делителями Метод Ферма выигрывает когда $p \approx q \approx \sqrt{n}$

Выводы

- Оба алгоритма успешно реализованы и протестированы
- ρ**-метод Полларда** показал высокую скорость на числах с малыми делителями
- ***Метод квадратов Ферма** эффективен когда делители близки друг к другу
- Выбор алгоритма зависит от структуры разлагаемого числа

Спасибо за внимание!