Лабораторная работа 12

Составить программу вычисления символов Якоби

Цель работы – используя алгоритм для вычисления символа Якоби, составить программу вычисления символа Якоби.

Задание к работе

В программной реализации рассмотренных ниже алгоритмов должен быть разработан интерфейс, удобный для эксплуатации. В интерфейсе следует предусмотреть:

- ввод начальной информации;
- вывод результатов расчета.

Разработать тестовые примеры для рабы с программой. Подготовить отчет по работе. В отчете описать алгоритмы проверки числа на простоту, описать структуру представления данных в программе, основные функции программы, назначение функций, входные и выходные параметры функций.

Теоретический материал

Символ Якоби

Определение. Пусть нечетное число p имеет следующее разложение на простые множители

$$p = p_1 p_2 \ldots p_k,$$

где $p_j, j \le k$, – простые числа, среди которых могут быть одинаковые. **Символ Якоби** $J(a, p)$ определяется равенством

$$J(a, p) = L(a, p_1)\, L(a, p_2) \ldots\, L(a, p_k),$$

где $L(a, p_i)$ символ Лежандра.

Заметим, что символ Лежандра является частным случаем символа Якоби. Более того, если число p является простым, то символ Якоби, по определению является символом Лежандра. Вместе с тем символ Якоби $J(a,p)$ может равняться единице, ($J(a, p) = 1$), а сравнение

$$x^2 \equiv a \bmod p$$

не имеет решений.

Пример. Определим символ Якоби $J(2, 15)$. По определению имеем

$$J(2, 15) = L(2,3)L(2,5).$$

Вычислим

$$L(2, 3) = [-1]^{(\alpha-1)/8} = [-1]^1 = -1,$$
$$\alpha = p^2 = 3^2 = 9$$

и

$$L(2, 5) = [-1]^{(\alpha-1)/8} = [-1]^3 = -1,$$
$$\alpha = p^2 = 5^2 = 25.$$

Окончательно получаем

$$J(2, 15) = L(2,3)L(2,5) = (-1)(-1) =1.$$

Итак, $J(2, 15) = 1$, а сравнение

$$x^2 \equiv 2 \ mod \ 15$$

не имеет решений.

Приведем основные свойства символа Якоби.

1. Если

$$a \equiv b \ mod \ p,$$

то

$$J(a, p) = J(b, p).$$

2. $J(a_1 \times a_2 \times \ldots \times a_k) = J(a_1, p) \times J(a_2, p) \times \ldots \times J(a_k, p)$.
3. $J(a^2, p) = 1$.
4. $J(1, p) = 1$.
5. $J(-1, p) = (-1)^{(p-1)/2} \ mod \ p$.
6. $J(2, p) = (-1)^{(p^2-1)/8}$.
7. $J(q, p) = -1^{[(p-1)/2][(q-1)/2]} L(p,q)$ – закон взаимности. Этот закон можно записать в виде

$$J(q, p)J(p, q) = -1^{[(p-1)/2][(q-1)/2]}.$$

Алгоритм вычисления символа Якоби

1. Если число a отрицательно, то выделяем множитель $J(-1, p)$;
2. Заменяем число a на остаток от деления числа a на p;
3. Если число a четно, представляем его в виде

$$a = 2^t a_1,$$

где a_1 – нечетное число.

4. Переходим к разложению

$$J(a, p) = J(2, p)^t \, J(a_1, p);$$

5. Отбрасываем множитель $J(2, p)^t$, если t – четное число;
6. Если t нечетно, то вычисляем символ Лежандра $J(2, p)^t$;
7. Применяем к $J(q, p)$ закон взаимности

$$L(q, p) = -1^{[(p-1)/2][(q-1)/2]} L(p,q).$$

Здесь полагается, что $q = a_1$.
8. Переходим на шаг 1.

Пример. Вычислить $J(506, 1103)$, здесь $a = 506$, $p = 1103$ – простое число. Так как 1103 – простое число, то значение символа Якоби равно значению символу Лежандра, т.е.

$$J(506, 1103) = L(506, 1103).$$

Однако вычисление символа Якоби упрощается за счет того, что при составном числе a можно применять закон взаимности, а при рассмотрении символов Лежандра составное число a надо раскладывать на произведение простых множителей. Что является не простой задачей.

Вычисляем $J(506, 1103)$.

1. При $a > 0$ множитель $J(-1, 1103)$ отсутствует;
2. Так как $506 < 1103$, то остаток равен самому числу;
3. Число $a = 506$ представляем в виде $506 = 2 \times 253$;
4. Переходим к разложению

$$J(506, 1103) = J(2, 1103) \, J(253, 1103);$$

5. Показатель степени множителя $J(2, 1103)^t = 1$ нечетно, поэтому переходим к шагу 6;
6. Вычисляем

$$J(2, 1103) = [-1]^{(\alpha-1)/8} = [-1]^{152076} = 1,$$

где

$$\alpha = p^2 = 1103^2;$$

7. Для множителя $J(253, 1103)$, применяя закон взаимности для a=253 и p=1103. Получаем

$$J(253, 1103) = (-1)^{126 \times 551} J(1103, 253) = \\ = J(1103, 253).$$

8. В итоге имеем $J(506, 1103) = J(1103, 253)$. Далее переходим на шаг 1 и начинаем вычислять $J(1103, 253)$, здесь $a = 1103$, $p = 253$;

Вычисляем $J(1103, 253)$.

1.При $a > 0$ множитель $J(-1, 253)$ отсутствует;

2. Остаток от деления числа 1103 на 253 равен 91, поэтому

$$J(1103, 253) = J(91, 253);$$

3. Число $a = 91$ – нечетное, переходим на шаг 7;

4. Не выполняется;

5. Не выполняется;

6. Не выполняется;

7. Для символа Якоби $J(91,253)$, применяя закон взаимности для a=91 и p=253. Получаем

$$J(91, 253) = (-1)^{45\times126}J(253,91) = \\ = J(253, 91).$$

8. В итоге имеем $J(1103, 253) = J(253, 91)$. Далее переходим на шаг 1 и начинаем вычислять $J(253, 91)$, здесь $a = 253$, $p = 91$;

Вычисляем $J(253, 91)$.

1. При $a > 0$ множитель $J(-1, 91)$ отсутствует;

2. Остаток от деления числа 253 на 91 равен 71, поэтому

$$J(253, 91) = J(71, 91);$$

3. Число $a = 71$ – нечетное, переходим на шаг 7;

4. Не выполняется;

5. Не выполняется;

6. Не выполняется;

7. Для символа Якоби $J(71, 91)$, применяя закон взаимности для a=71 и p=91. Получаем

$$J(71, 91) = (-1)^{35\times45}J(91, 71) = \\ = -J(91, 71).$$

8. В итоге имеем $J(253, 91) = -J(91, 71)$. Далее переходим на шаг 1 и начинаем вычислять $J(91, 71)$, здесь $a = 91$, $p = 71$;

Вычисляем $-J(91, 71)$.

1. При $a = 91 > 0$ множитель $J(-1, 71)$ отсутствует;

2. Остаток от деления числа 91 на 71 равен 20, поэтому

$$J(91, 71) = J(20, 71);$$

3. число $a = 20$ представим в виде $a = 2^2 \times 5$;

4. переходим к разложению

$$J(20, 71) = J(2, 71)^2 J(5, 71);$$

5. показатель степень у множителя $J(2, 71)$ t=2 четный, поэтому

$$J(2, 71)^2 = 1.$$

Переходим к шагу 7;

6. Не выполняется;

7. Для символа Якоби $J(5, 71)$, применяя закон взаимности для a=5 и p=71, получаем

$$J(5, 71) = (-1)^{2 \times 35} J(71, 5) = J(71, 5).$$

8. В итоге имеем $-J(91, 71) = -J(71, 5)$. Далее переходим на шаг 1 и начинаем вычислять $-J(71, 5)$, здесь $a = 71$, $p = 5$;

Вычисляем $-J(71, 5)$.

1. При $a = 71 > 0$ множитель $J(-1, 71)$ отсутствует;

2. Остаток от деления числа 71 на 5 равен 1, поэтому

$$J(71, 5) = J(1, 5);$$

3. Число $a = 1$ – нечетное, переходим на шаг 7;

4. Не выполняется;

5. Не выполняется;

6. Не выполняется;

7. Вычисляем символ Якоби $J(1, 5) = 1$.

8. В итоге имеем $-J(71, 5) = -1$. Вычисление символа Якоби $J(1103, 253)$ завершен. Окончательно получаем $J(1103, 253) = -1$. Значение символа Якоби

$$J(506,1103) = -1$$

позволяет сделать вывод, что сравнение

$$x^2 \equiv 506 \ mod \ 1103$$

не имеет решений.