**Подготовил Кудинов Антон Александрович, ЕТ-225**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

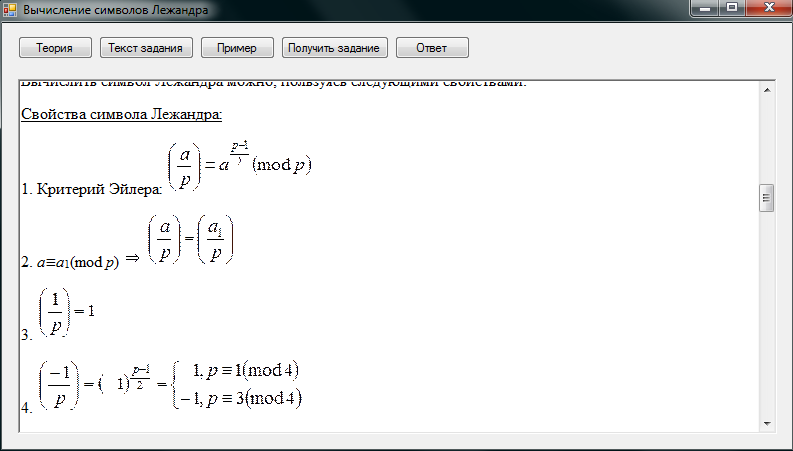
**Лабораторная работа «Вычисление символов Лежандра»**

## Общая информация

Необходимо разработать модуль лабораторной работы «Вычисление символов Лежандра».

Окно лабораторной работы должно иметь собственно основное окно, и 5 кнопок (см. рисунок 1):

1. теория;
2. текст задания;
3. пример выполнения задания;
4. получение задания;
5. проверка ответа.



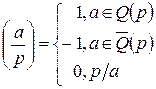
Рисунок

Кнопки «Теория», «Текст задания» и «Пример» изменяют содержание основного окна на содержимое соответствующих им блоков. Кнопка «Получить задание» должна вызывать стандартное диалоговое окно выбора папки. Кнопка «Ответ» вызывает содержимое блока «Ответ» в отдельной форме. По умолчанию основное окно отображает блок «Теория».

## Блоки «Теория», «Текст задания» и «Пример»

Здесь приведено описание блоков теоретического материала, текста задания и примера выполнения.

**Текст блока «Теория»**

Символом Лежандра называется символ (читается «символ Лежандра *а* по *р*»). *а* называется числителем, *р* – знаменателем символа Лежандра. Символ Лежандра отвечает на вопрос, является ли число *а* квадратичным вычетом по модулю *р*. Если *a* = 1, то *a* является квадратичным вычетом, если *a* = -1, то *a* является квадратичным невычетом.

Вычислить символ Лежандра можно, пользуясь следующими свойствами.

**Свойства символа Лежандра:**

1. Критерий Эйлера: https://helpiks.org/helpiksorg/baza6/90407071027.files/image463.gif

2. *a≡a*1(mod *p*) https://helpiks.org/helpiksorg/baza6/90407071027.files/image364.gifhttps://helpiks.org/helpiksorg/baza6/90407071027.files/image466.gif

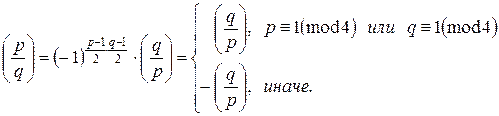
3. https://helpiks.org/helpiksorg/baza6/90407071027.files/image468.gif

4. https://helpiks.org/helpiksorg/baza6/90407071027.files/image470.gif

5. https://helpiks.org/helpiksorg/baza6/90407071027.files/image472.gif

6. https://helpiks.org/helpiksorg/baza6/90407071027.files/image474.gif

7. https://helpiks.org/helpiksorg/baza6/90407071027.files/image476.gif

8. 3акон взаимности: если *p*, *q* – нечетные простые числа https://helpiks.org/helpiksorg/baza6/90407071027.files/image348.gif

где *ps(i),s(i+1)* — вероятность, что после символа *s(i)* следует символ *s(i+1)*. Эта формула удобна для теоретического анализа, однако, при практической реализации при большом количестве умножений мантисса переполняется и удобнее вместо произведения использовать, например, сумму.

Алгоритм вычисления символа Лежандра

1. Если число *a* отрицательно, то выделяем множитель *L(-1, p)*;
2. Заменяем число *a* на остаток от деления числа *a* на *p*;
3. Раскладываем число *a* в произведение в простых сомножителей если число на простые множители не разлагается, то переходим на шаг 4;
4. Переходим к разложению ;
5. Отбрасываем множители с четным значением показателя *j*, *j* *k*;
6. Вычисляем символ Лежандра для *aj* = 2;
7. Если все символы Лежандра в выражении вычислены, то алгоритм вычисления L(a,p) завершаем. В противном случае для множителей , у которых *aj* 2, применяем закон взаимности .Здесь полагается, что *p = aj*.
8. Переходим к шагу 1.

**Текст блока «Текст задания»**

**Задание на лабораторную работу**

Вычислить символы Лежандра и раскодировать сообщение, учитывая, что исходный текст – текст на русском языке в кодировке *cp861* и при кодировании нулевой бит заменялся квадратичным невычетом, а единичный – квадратичным вычетом.

**Порядок действий**

1. Вычислить заданные символы Лежандра.
2. Раскодировать исходное сообщение.

**Текст блока «Пример»**

a) https://helpiks.org/helpiksorg/baza6/90407071027.files/image492.gif

Следовательно, 10 – квадратичный вычет по модулю 13.

б) https://helpiks.org/helpiksorg/baza6/90407071027.files/image494.gif

https://helpiks.org/helpiksorg/baza6/90407071027.files/image496.gif.

Следовательно, 1350 является квадратичным невычетом по модулю 1381.

**Интерфейс блоков «Теория» и «Текст задания»**

Данные блоки имеют одинаковый вид интерфейса –– окно, содержащее текст блока (с картинками). Текстовое окно должно иметь фиксированный размер и бегунок для вмещения содержания, превышающего по размеру само окно. Ввиду того, что содержимое основного окна программы меняется при нажатиях верхних кнопок, то дополнительных элементов для данных трех блоков не требуется.

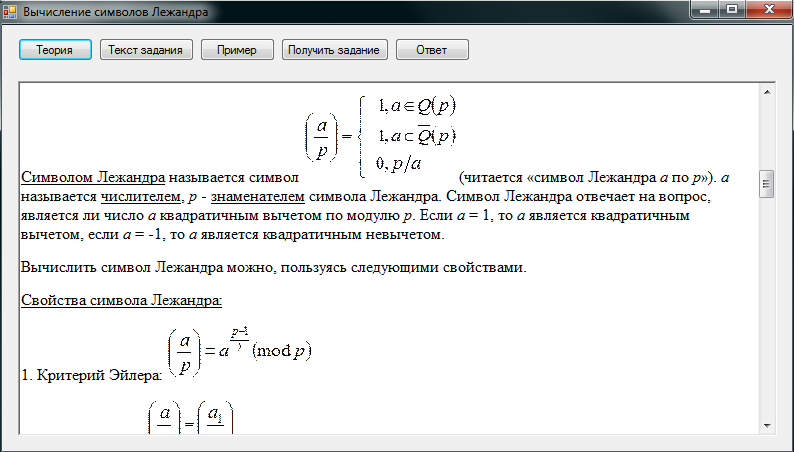


Рисунок 2

## Блок «Получение задания»

Блок должен содержать кнопку «Получить задание», при нажатии на которую вызывается диалог выбора папки, в которую пользователь желает сохранить задание (см. рисунок 3). Если путь для сохранения неверен или пуст, необходимо выдавать соответствующие сообщения.

Выдаваемое задание должно соответствовать году обучения, семестру и номеру бригады, выбранных в главном меню.

Каждый экземпляр задания должен быть однозначно сгенерирован генератором псевдослучайных чисел на основании года, семестра и номера бригады, чтобы было возможно однозначно восстановить этот экземпляр для проверки.

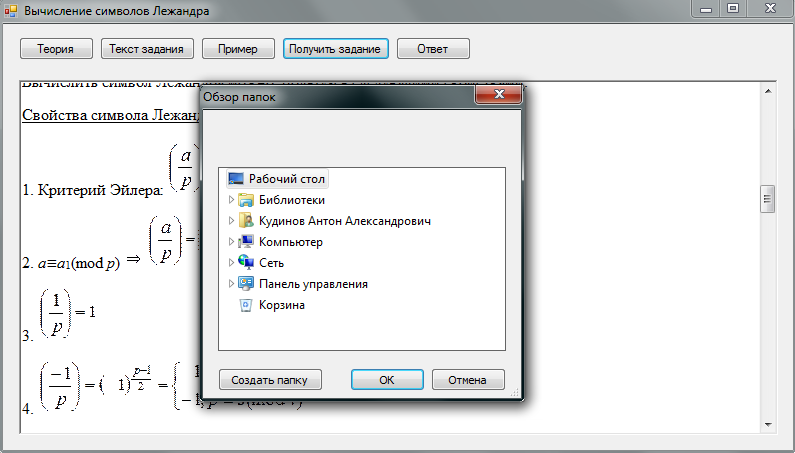


Рисунок 3

Алгоритм генерации содержания каждого экземпляра задания следующий:

1. выбрать случайным образом отрывок текста на русском языке (допустима только кириллица и знак «пробел») из ресурсов проекта, а именно – из файла Sholohov.txt. Отрывок должен быть взят таким образом, чтобы первый символ отрывка был началом слова, а длина отрывка составила 30 символов + окончание последнего слова;
2. закодировать каждый символ отрывка соответствующим значением из кодировки *cp866;*
3. перевести полученные значения в двоичный код длиной 8 бит на символ таким образом, чтобы начальные нулевые биты каждого значения не были выброшены из его двоичной записи;
4. для каждого бита полученного кода сгенерировать символ Лежандра таким образом, что
5. *p* для каждого из символов на один экземпляр задания будет иметь одинаковую длину, составляющую не менее 10 цифр;
6. все *a* были различны между собой;
7. для каждого нулевого бита полученного кода генерируется такой символ Лежандра, результатом вычисления которого является квадратичный невычет, а для каждого единичного бита – такой символ Лежандра, результатом вычисления которого является квадратичный вычет;
8. заменить каждый бит полученного кода на соответствующий ему символ Лежандра;
9. составить столбец из последовательности полученных символов Лежандра, где каждый символ представлен в виде «*L(a,p)=?*».

Символы отрывка и расшифрованного текста должны быть в верхнем регистре.

Заданием, которое выдаётся пользователю, является полученный столбец из символов Лежандра.

## Блок «Проверка ответа»

Блок проверки должен содержать поля для ввода текста, а также кнопку «Проверить ответ» (см. рисунок 4), при нажатии на которую вызывается процедура проверки, после чего пользователь уведомляется о правильности/неправильности ответа.

Ответом задания является расшифрованный текст.

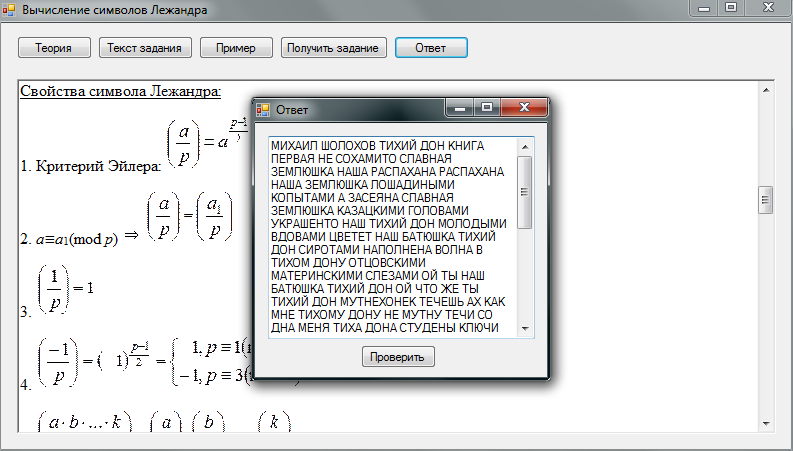


Рисунок 4

Если он соответствует выбранному при генерации задания отрывку, то задание выполнено верно/неверно, и это отображается в соответствующем окошке (см. рисунок 5). В строке ответа необходимо убирать все символы, кроме заглавных букв русского алфавита. Также необходимо убирать все лишние пробелы в конце и в начале строки.

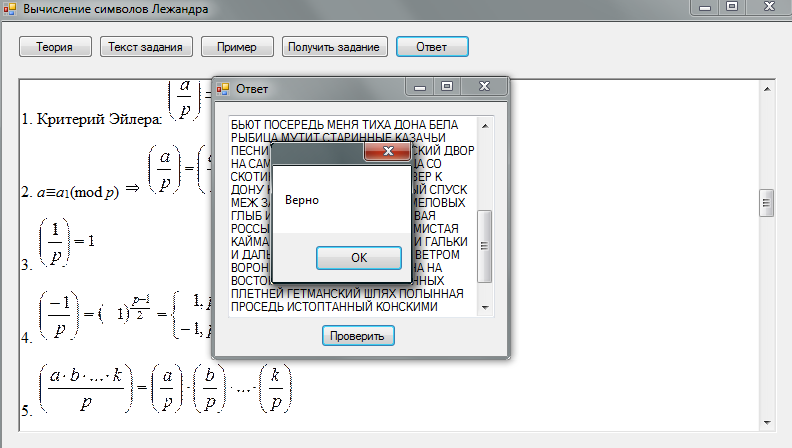


Рисунок 5

## Требования к тестированию

При тестировании разработанной программы необходимо обработать следующие исключительные ситуации:

1. Для блока «Получение задания»:

* выход за пределы общего текста при выборе отрывка для генерации задания;
* несуществующий путь для ввода полученного задания;
* незаданный путь для ввода полученного задания;

1. Для блока «Проверка ответа»:

* выход за пределы общего текста при генерации правильного ответа;
* лишние символы при сравнении строки ответа студента и правильного ответа.

При несуществующем или незаданном пути пользователю должны быть выведены соответствующие сообщения.

Выход за пределы общего текста должен быть предотвращен на этапе разработки программы.

При сравнении строки ответа студента и правильного ответа все лишние символы (указанные в пункте 4) в строке ответа должны быть исключены.

## Требования к программной документации

Для создания программной документации необходимо разработать руководство пользователя на основе «ГОСТ 19.505-79. ЕСПД. Руководство оператора. Требования к содержанию и оформлению». Это руководство должно включать в себя следующие разделы:

* назначение программы;
* условия выполнения программы;
* выполнение программы;
* сообщения пользователю.