

Язык ассемблера - язык низкого уровня, команды которого обычно соответствуют командам процессора. Относится к группе машинно-зависимых языков.



Для создания заготовки программы в RadASM необходимо создать новый проект, выбрать ассемблер, тип и шаблон проекта, типы создаваемых файлов и пункты меню необходимые для работы с проектом.

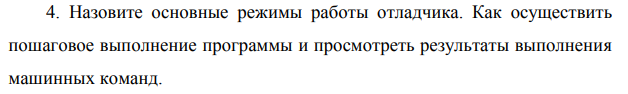
Заготовка содержит:

* указание настроек для транслятора, подключение описаний процедур и библиотек
* разделы объявления констант и переменных
* сегмент кода, завершающийся вызовом ExitProcess



Чтобы запустить программу, необходимо пройти следующие этапы обработки:

* Трансляцию(ассемблирование) - программа преобразуется из мнемонических (словесных) команд в машинные (двоичные)
* Компоновка - к двоичному коду основной программы добавляются объектные коды используемых подпрограмм
* Запустить программу/ запустить программу в режиме отладки

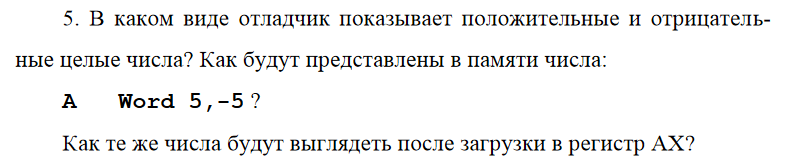


Основные режимы работы отладчика - с заходом и без захода в тело процедуры.

Для начала отладки необходимо транслировать и скомпоновать программу, затем выбрать опцию Run w debug.

Далее для выполнения шага с заходом в процедуру необходимо нажимать F7, без захода - F8.

Коды машинных команд видны в левом верхнем углу, содержимое памяти - в левом нижнем, содержимое регистров и флагов - в правом верхнем, стека - в правом нижнем.



5 => 05 00

-5 => FB FF

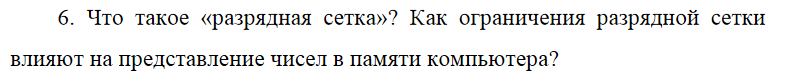
В регистре AX:

510 => 00 0516

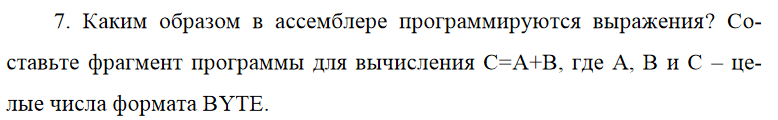
-510 => FF FB16 = 11111111 11111111 11111111 111110112 - дополнительный код -5

В памяти байты чисел представлены в обратном порядке, отрицательные числа хранятся в дополнительном коде.

В регистре байты становятся в прямой порядок.



Под разрядной сеткой понимают количество разрядов, выделенное в ЭВМ под запись 1 числа. Разрядная сетка определяет диапазон значений для целых чисел (причем для чисел со знаком он в 2 раза меньше чем для чисел без знака той же разрядности) и точность для дробных чисел.



Любое математическое выражение в ассемблере имеет не более двух операндов, поэтому любое сложное выражение необходимо разбивать на последовательность простых.

Фрагмент программы:

.Data

A BYTE 1

B BYTE 4

.Data?

C BYTE ?

.CODE

Start:

mov AX, A

add AX, B

mov C, AX

Вывод: в ходе работы были изучены основы работы со средой RadAsm, отладчиком OllyDbg, основы программирования на языке ассемблера(объявление переменных и констант, команда MOV, запуск программы), особенности внутреннего представления данных.