

LAB 04

Working with Data related Operator and Directives, Addressing



STUDENT NAME

ROLL NO

SEC

LAB ENGINEER'S SIGNATURE & DATE

MARKS AWARDED: /

NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCES
(NUCES), KARACHI

Prepared by: Qurat ul ain & Rabia Ansari

Lab Session 04: Working with Data Related Operators and Directives, Addressing

OBJECTIVES:

- Observing effect of Arithmetic Instructions on Flag Register
- Direct-offset operands
- OFFSET operator
- PTR operator
- TYPE operator
- LENGTHOF operator
- SIZEOF operator
- Indirect operands
- Indexed operands

Effect of Arithmetic Instructions on Flag Registers

- Status flags are updated to indicate certain properties of the result
- Once a flag is set, it remains in that state until another instruction that affects the flags is executed

Z-Zero Flag:

The Zero flag is set when the result of an operation produces zero in the destination operand.

```
mov cx,1
sub cx,1          ; CX = 0, ZF = 1
mov ax,0FFFFh
inc ax            ; AX = 0, ZF = 1
inc ax            ; AX = 1, ZF = 0
```

Remember...

- A flag is **set** when it equals 1.
- A flag is **clear** when it equals 0.

C-Carry Flag:

This flag is set, when there is a carry out of MSB in case of addition and borrow in case of subtraction.

The Carry flag is set when the result of an operation generates an unsigned value that is out of range (too big or too small for the destination operand).



```

mov al,0FFh
add al,1                ; CF = 1, AL = 00

; Try to go below zero:

mov al,0
sub al,1                ; CF = 1, AL = FF

```

S-Sign Flag:

This flag indicates the sign of the result of an operation. A 0 for positive number and 1 for a negative number.

<pre> mov AL, 15 add AL, 97 clears the sign flag as the result is 112 (or 0111000 in binary) </pre>	<pre> mov AL, 15 sub AL, 97 sets the sign flag as the result is -82 (or 10101110 in binary) </pre>
---	--

AC-Auxiliary Carry Flag:

This flag is set, if there is a carry from the lowest nibble, i.e., bit three during addition, or borrow for the lowest nibble, i.e. bit three, during subtraction.

Suppose we add 1 to 0Fh. The sum (10h) contains a 1 in bit position 4 that was carried out of bit position 3:

```

mov al,0Fh
add al,1                ; AC = 1

```

P Parity Flag:

The Parity flag (PF) is set when the least significant byte of the destination has an even number of 1 bits. The following ADD and SUB instructions alter the parity of AL:

```

mov al,10001100b
add al,00000010b        ; AL = 10001110, PF = 1
sub al,10000000b        ; AL = 00001110, PF = 0

```

O-Over flow Flag:



The Overflow flag is set when the result of a signed arithmetic operation over-flows or

underflows the destination operand. For example, the largest possible integer signed byte value is +127; adding 1 to it causes overflow:

```
mov al,+127
add al,1           ; OF = 1
```

Similarly, the smallest possible negative integer byte value is 128. Subtracting 1 from it causes underflow. The destination operand value does not hold a valid arithmetic result, and the Overflow flag is set:

```
mov al,-128
sub al,1           ; OF = 1
```

Direct-offset Operands:

You can add a displacement to the name of a variable, creating a direct-offset operand.

Example:

```
.data
arrayB          BYTE
10h,20h,30h,40h,50h  arrayW
WORD 100h,200h,300h

.code
mov al,arrayB      ; AL = 10h
mov al,[arrayB+1]   ; AL = 20h
mov ax,arrayW       ; AX = 100h
mov ax,[arrayW+2]    ; AX = 200h
```

Similarly, the second element in a doubleword array is 4 bytes beyond the first one.

DATA-RELATED OPERATORS AND DIRECTIVES

OFFSET Operator:

The OFFSET operator returns the offset of a data label.

Syntax:

MOV reg32, OFFSET mem ; reg32 points to count



Example:

```
.data
bVal BYTE ?
wVal WORD ?
dVal DWORD ?
dVal2 DWORD ?
```

If bVal is located at offset 00404000h, we would get:

```
mov esi, OFFSET bVal      ; ESI = 00404000
mov esi, OFFSET wVal      ; ESI = 00404001
mov esi, OFFSET dVal      ; ESI = 00404003
mov esi, OFFSET dVal2     ; ESI = 00404007
```

PTR Operator:

We can use the PTR operator to override the declared size of an operand. Note PTR must be used in combination with one of the standard assembler data types.

For example, that we would like to move the lower 16 bits of a doubleword variable named myDouble into AX. The assembler will not permit the following move because the operand sizes do not match:

```
.data
myDouble DWORD 12345678h
.code
mov ax, myDouble    ; error
```

But the WORD PTR operator makes it possible to move the low-order word (5678h) to AX:

```
mov ax, word ptr myDouble      ; AX = 5678H
```

and higher word (1234h) to AX:

```
mov dx, word ptr myDouble+2    ; DX = 1234H
```

Moving Smaller Values into Larger Destinations

We might want to move two smaller values from memory to a larger destination operand. In the next example, the first word is copied to the lower half of EAX and the second word is copied to the upper half.

The DWORD PTR operator makes this possible:



```
.data
wordList WORD 5678h, 1234h
.code
mov eax, DWORD PTR wordList           ; EAX = 12345678h
```

TYPE Operator:

The TYPE operator returns the size, in bytes, of a single element of a variable.

Syntax:

MOV reg16, TYPE mem

Example 1:

```
.data
var1 BYTE ?      ; TYPE var1 = 1
var2 WORD ?      ; TYPE var2 =
2 var3 DWORD ?   ; TYPE var3 =
4 var4 QWORD ?   ; TYPE var4 = 8
```

Example 2:

```
.data
var1 BYTE 20h
var2     WORD
1000h     var3
DWORD ?
var4 BYTE 10, 20, 30, 40, 50
msg BYTE 'File not found', 0
.code
mov ax, type var1      ; AX = 0001
mov ax, type var2      ; AX = 0002
mov ax, type var3      ; AX = 0004
mov ax, type var4      ; AX = 0001
mov ax, type msg       ; AX = 0001
```

LENGTHOF Operator:

The LENGTHOF operator counts the number of individual elements in a variable that has been defined using DUP.

Syntax:



MOV reg16 , LENGTHOF mem

Example:

```
.data
val1 WORD 1000h
val2 SWORD 10, 20, 30
array WORD 10 DUP(?),0
array2 WORD 5 DUP(3 DUP(0))
message BYTE 'File not found', 0

.code
mov ax, LENGTHOF val1 ; AX =1
mov ax, LENGTHOF val2 ; AX =3
mov ax, LENGTHOF array ; AX = 11 mov
ax, LENGTHOF array2 ; AX = 15 mov ax,
LENGTHOF message ; AX = 15
```

SIZEOF Operator:

The SIZEOF operator returns the number of bytes an array takes up. It is similar in effect to multiplying LENGTHOF with TYPE.

Syntax:

MOV reg16/32 , SIZEOF mem

Example:

```
.data
intArray WORD 32 DUP(0)
.code
mov eax,SIZEOF intArray ; EAX = 64
```

Indirect Operands

In protected mode, an indirect operand can be any 32-bit general-purpose register (EAX, EBX, ECX, EDX, ESI, EDI, EBP, and ESP) surrounded by brackets. The register is assumed to contain the address of some data.

Example:

```
.data
byteVal BYTE 10h
.code
mov esi,OFFSET byteVal
mov al,[esi] ; AL = 10h
```



If the destination operand uses indirect addressing, a new value is placed in memory at the location pointed to by the register.

```
mov [esi],bl
```

Using PTR with Indirect Operands

```
inc [esi] ; error: operand must have size
```

The assembler does not know whether ESI points to a byte, word, doubleword, or some other size. The PTR operator confirms the operand size:

```
inc BYTE PTR [esi]
```

Arrays

Indirect operands are ideal tools for stepping through arrays.

Example:

```
.data
```

```
arrayB BYTE 10h,20h,30h
```

```
.code
```

```
mov esi,OFFSET arrayB
```

```
mov al,[esi] ; AL = 10h
```

```
inc esi
```

```
mov al,[esi] ; AL = 20h
```

If we use an array of 16-bit integers, we add 2 to ESI to address each subsequent array element.

```
.data
```

```
arrayW WORD 1000h,2000h,3000h
```

```
.code
```

```
mov esi,OFFSET arrayW
```

```
mov ax,[esi] ; AX = 1000h
```

```
add esi,2
```

```
mov ax,[esi] ; AX = 2000h
```



If we use an array of 32-bit integers, we add 4 to ESI to address each subsequent array element.

Indexed Operands

An indexed operand adds a constant to a register to generate an effective address. Any of the 32-bit general-purpose registers may be used as index registers.

SYNTAX:

constant [reg32] ; reg32 can be any of the 32-bit general registers

[constant + reg32]

EXAMPLE:

```
.data
```

```
arrayB BYTE 20, 40, 60, 80
```

```
.code
```

```
mov esi, 1
```

```
mov al, arrayB[esi]
```

```
inc esi
```

```
mov al, arrayB[esi]
```

```
mov esi, 3
```

```
mov al, [arrayB + esi]
```

Adding Displacements: The second type of indexed addressing combines a register with a constant offset. The index register holds the base address of an array.

```
INCLUDE Irvine32.inc
```

```
.data
```

```
arrayW WORD 1000h,2000h,3000h
```

```
.code
```

```
main PROC
```

```
mov eax,0
```

```
mov ebx,0
```

```
mov ecx,0
```



```
mov esi,OFFSET arrayW  
mov ax,[esi] ; AX = 1000h  
mov bx,[esi+2] ; AX = 2000h  
mov cx,[esi+4] ; AX = 3000h
```

Scale Factors in Indexed Operands

Indexed operands must take into account the size of each array element when calculating offsets.

SYNTAX:

constant [reg32 * TYPE constant]

EXAMPLE:

```
INCLUDE Irvine32.inc
```

```
.data
```

```
arrayW WORD 1000h, 2000h, 3000h, 4000h
```

```
.code
```

```
main PROC
```

```
mov eax,0
```

```
mov ebx,0
```

```
mov ecx,0
```

```
mov esi, 1
```

```
mov ax, arrayW[esi * TYPE arrayW]
```

```
mov esi, 2
```

```
mov bx, arrayW[esi * TYPE arrayW]
```

```
mov esi, 3
```

```
mov cx, arrayW[esi * TYPE arrayW]
```



call DumpRegs

Exercises:

1. Declare a 32-bit signed integer `val1` and initialize it with the eight thousand. If `val1` is incremented by 1 using the `ADD` instruction, what will be the values of the Carry and Sign flags?
2. Write down the values of the Carry, Sign, Zero, and Overflow flags after each instruction has executed:

```
mov ax,7FF0h
add al,10h      ; a. CF = SF = ZF = OF =
add ah,1        ; b. CF = SF = ZF = OF =
add ax,2        ; c. CF = SF = ZF = OF =
```

3. Initialize a double word array consisting of elements 8, 5, 1, 2, 6. Sort the given array in ascending order directly with the help of registers. Use direct-offset addressing to access the elements.
4. Use following array declarations:
`arrayB BYTE 10, 20, 30`
`arrayW WORD 150, 250, 350`
`arrayD DWORD 600, 1200, 1800`

Now initialize three double word variables `SUM1`, `SUM2`, `SUM3` and perform following operations (expressed in pseudo-code here):

`SUM1 = arrayB[0] + arrayW[0] + arrayD[0]`

`SUM2 = arrayB[1] + arrayW[1] + arrayD[1]`

`SUM3 = arrayB[2] + arrayW[2] + arrayD[2]`

5. Initialize two arrays:
`array1 BYTE 10, 20, 30, 40`
`array2 BYTE 4 DUP (?)`

Copy elements of `array1` into `array2` in reverse order using either indirect addressing or direct-offset addressing.

6. Subtract an array of 5 doublewords using indirect operands.
7. Use following array declarations:



arrayB BYTE 60, 70, 80

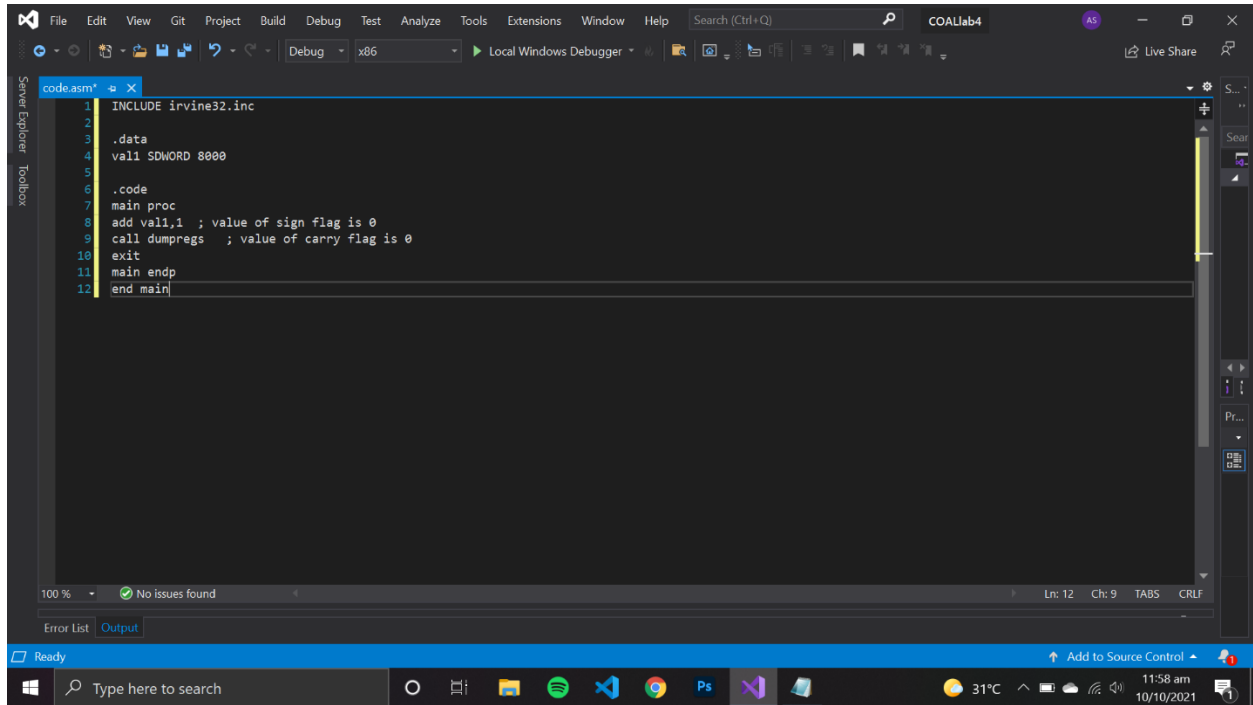
arrayW WORD 150, 250, 350

arrayD DWORD 600, 1200, 1800

For each array, add its 1st and last element using scale factors and display the result in a separate register.



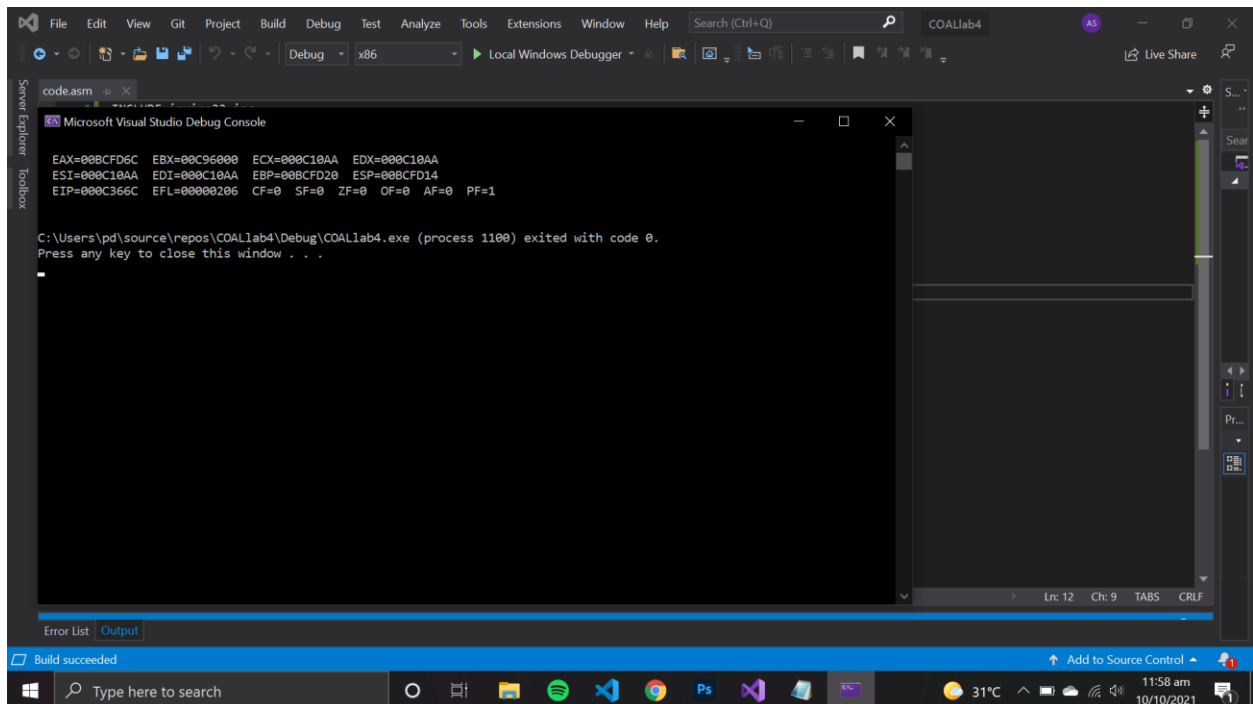
TASK 1:



```
1 INCLUDE irvine32.inc
2
3 .data
4 val1 SDWORD 8000
5
6 .code
7 main proc
8 add val1,1 ; value of sign flag is 0
9 call dumpregs ; value of carry flag is 0
10 exit
11 main endp
12 end main
```

100 % No issues found Ln: 12 Ch: 9 TABS CRLF

OUTPUT:

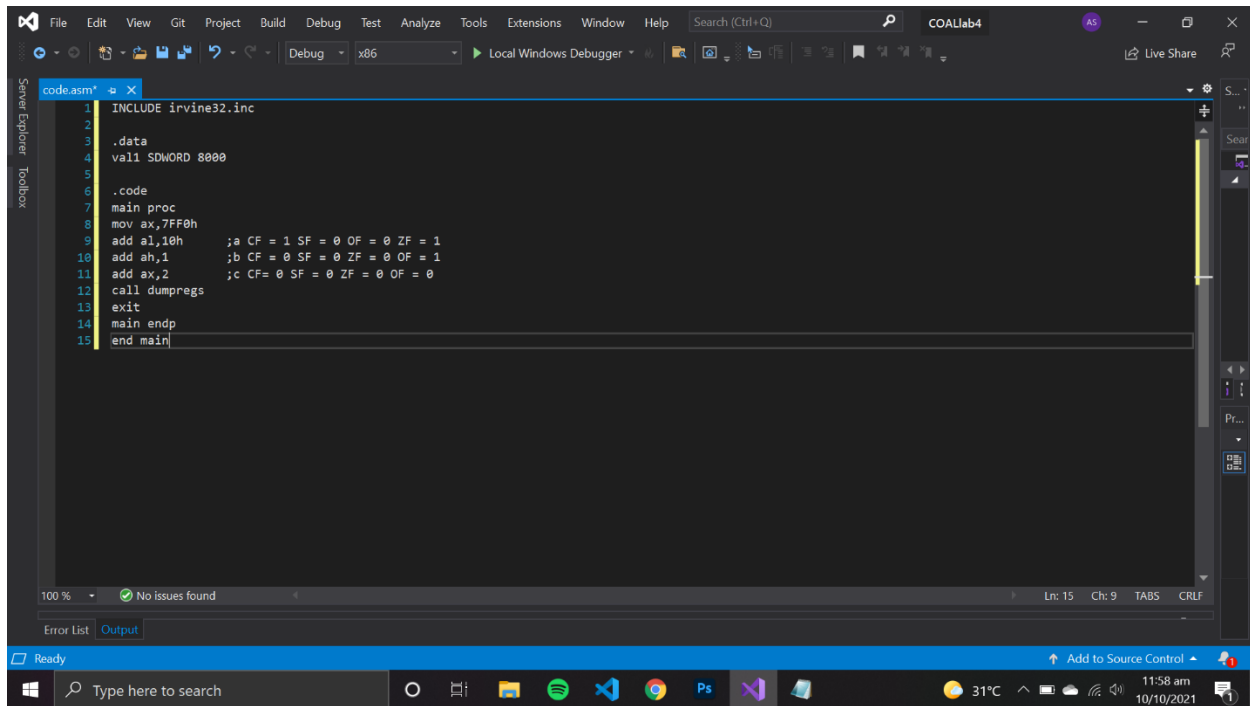


```
Microsoft Visual Studio Debug Console
EAX=00BCFD6C EBX=00C96000 ECX=000C10AA EDX=000C10AA
ESI=000C10AA EDI=000C10AA EBP=00BCFD20 ESP=00BCFD14
EIP=000C366C EFL=00000206 CF=0 SF=0 ZF=0 OF=0 AF=0 PF=1

C:\Users\pd\source\repos\COALLab4\Debug\COALLab4.exe (process 1100) exited with code 0.
Press any key to close this window . . .
```

Build succeeded

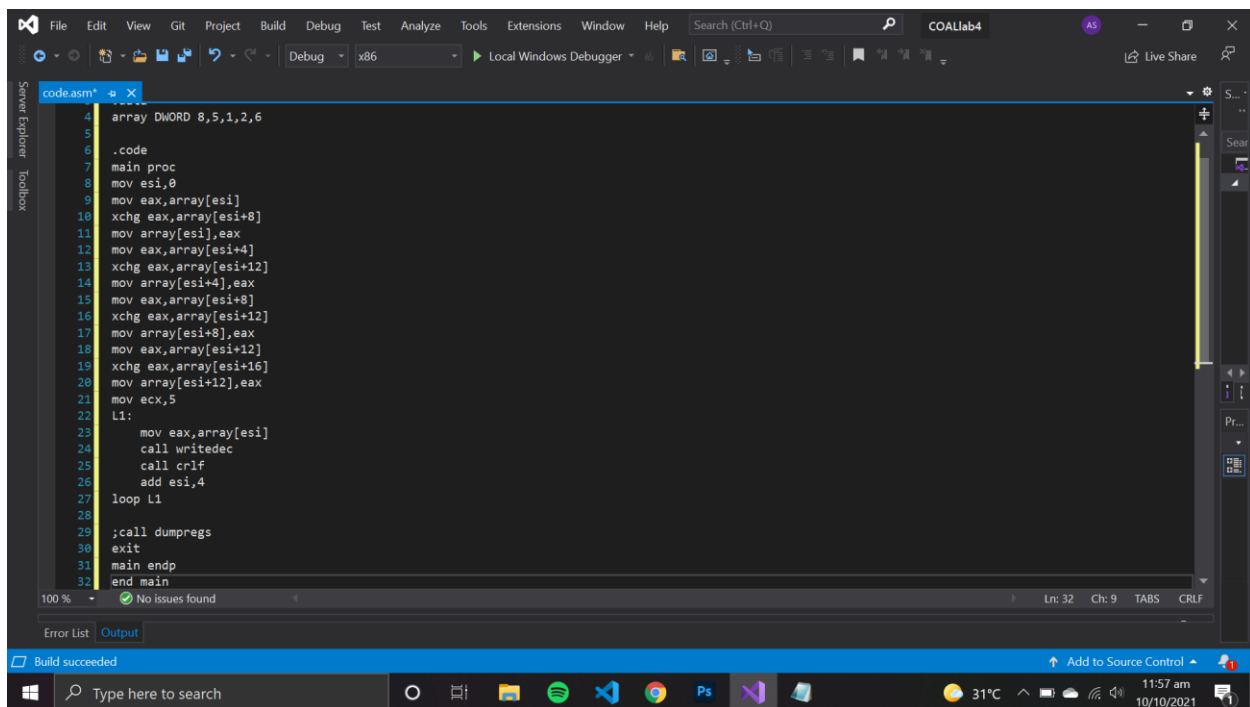
TASK 2:



The screenshot shows the Visual Studio Code editor with a file named `code.asm` open. The code is assembly for x86, using the Irvine32 library. It defines a data segment with a word `val1` set to `8000h`. The code segment contains a `main` procedure that initializes `ax` to `7FF0h`, then adds `10h` to `al`, `1` to `ah`, and `2` to `ax`. It then calls `dumpregs`, exits, and ends the main procedure. The status bar at the bottom indicates 'Ready' and 'No issues found'.

```
1 INCLUDE irvine32.inc
2
3 .data
4 val1 SDWORD 8000h
5
6 .code
7 main proc
8 mov ax,7FF0h
9 add al,10h    ;a CF = 1 SF = 0 OF = 0 ZF = 1
10 add ah,1     ;b CF = 0 SF = 0 ZF = 0 OF = 1
11 add ax,2     ;c CF = 0 SF = 0 ZF = 0 OF = 0
12 call dumpregs
13 exit
14 main endp
15 end main
```

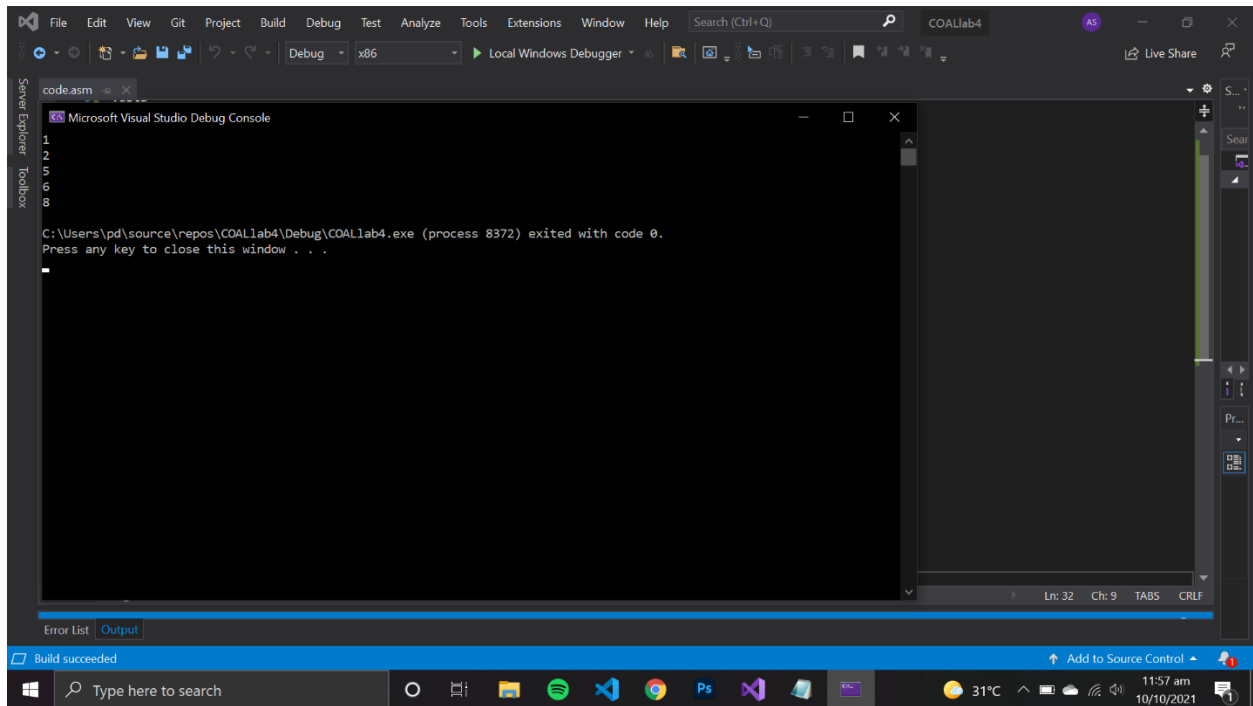
TASK 3



The screenshot shows the Visual Studio Code editor with a file named `code.asm` open. The code is assembly for x86, using the Irvine32 library. It defines a data segment with a word `array` containing the values `8, 5, 1, 2, 6`. The code segment contains a `main` procedure that initializes `esi` to `0`, then enters a loop where it swaps the values at `array[esi]` and `array[esi+8]`, increments `esi` by `4`, and repeats the process until `esi` reaches `5`. It then calls `dumpregs`, exits, and ends the main procedure. The status bar at the bottom indicates 'Build succeeded'.

```
4 array DWORD 8,5,1,2,6
5
6 .code
7 main proc
8 mov esi,0
9 mov eax,array[esi]
10 xchg eax,array[esi+8]
11 mov array[esi],eax
12 mov eax,array[esi+4]
13 xchg eax,array[esi+12]
14 mov array[esi+4],eax
15 mov eax,array[esi+8]
16 xchg eax,array[esi+12]
17 mov array[esi+8],eax
18 mov eax,array[esi+12]
19 xchg eax,array[esi+16]
20 mov array[esi+12],eax
21 mov ecx,5
22 L1:
23     mov eax,array[esi]
24     call writedec
25     call crlf
26     add esi,4
27     loop L1
28
29 ;call dumpregs
30 exit
31 main endp
32 end main
```

OUTPUT:

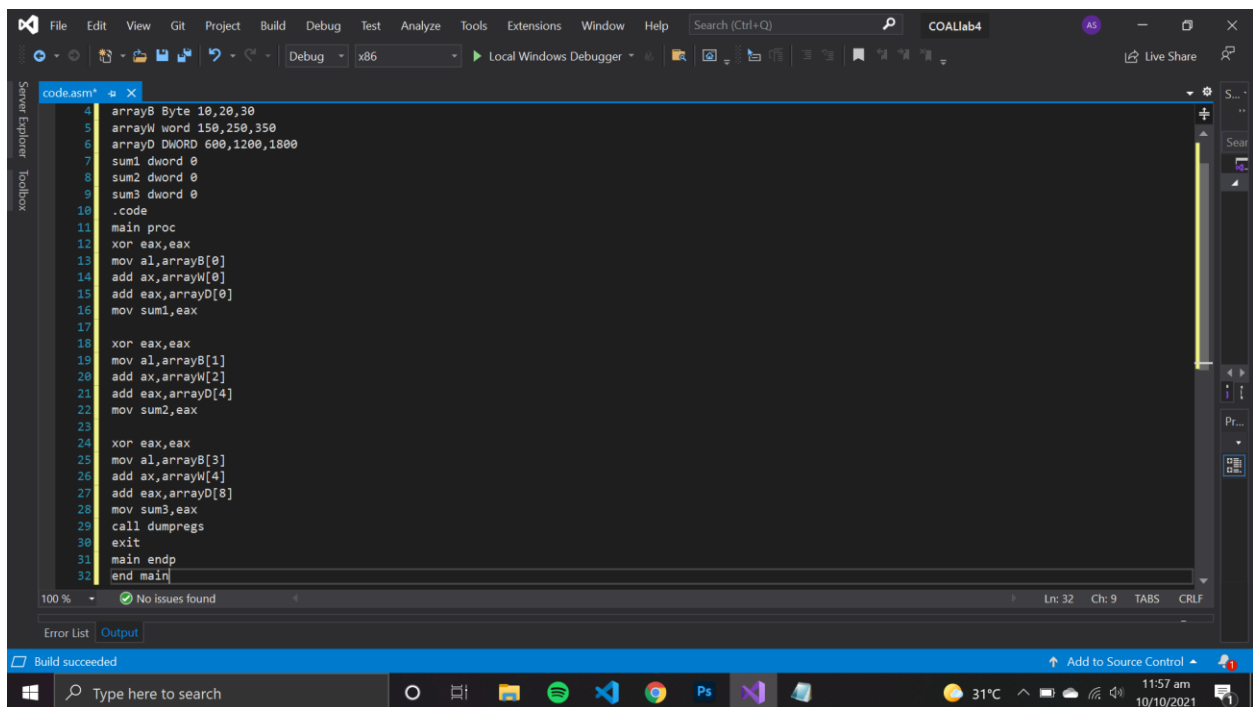


The screenshot shows the Visual Studio IDE with the 'Microsoft Visual Studio Debug Console' window open. The console displays the following text:

```
C:\Users\pd\source\repos\COALLab4\Debug\COALLab4.exe (process 8372) exited with code 0.  
Press any key to close this window . . .
```

The status bar at the bottom indicates 'Build succeeded'.

TASK 4:

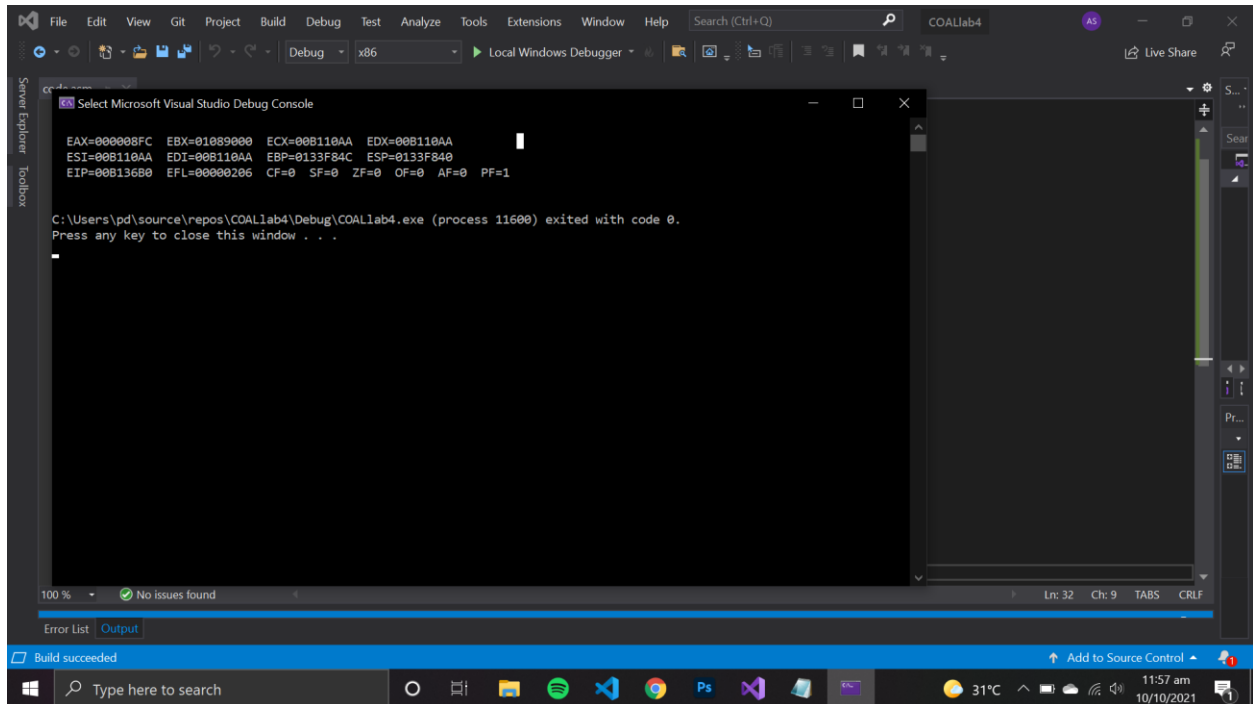


The screenshot shows the Visual Studio IDE with the assembly code for 'code.asm' open. The code is as follows:

```
4  array8 Byte 10,20,30  
5  arrayW word 150,250,350  
6  arrayD DWORD 600,1200,1800  
7  sum1 dword 0  
8  sum2 dword 0  
9  sum3 dword 0  
10 .code  
11 main proc  
12 xor eax,eax  
13 mov al,array8[0]  
14 add ax,arrayW[0]  
15 add eax,arrayD[0]  
16 mov sum1,eax  
17  
18 xor eax,eax  
19 mov al,array8[1]  
20 add ax,arrayW[2]  
21 add eax,arrayD[4]  
22 mov sum2,eax  
23  
24 xor eax,eax  
25 mov al,array8[3]  
26 add ax,arrayW[4]  
27 add eax,arrayD[8]  
28 mov sum3,eax  
29 call dumpregs  
30 exit  
31 main endp  
32 end main
```

The status bar at the bottom indicates 'Build succeeded'.

OUTPUT:

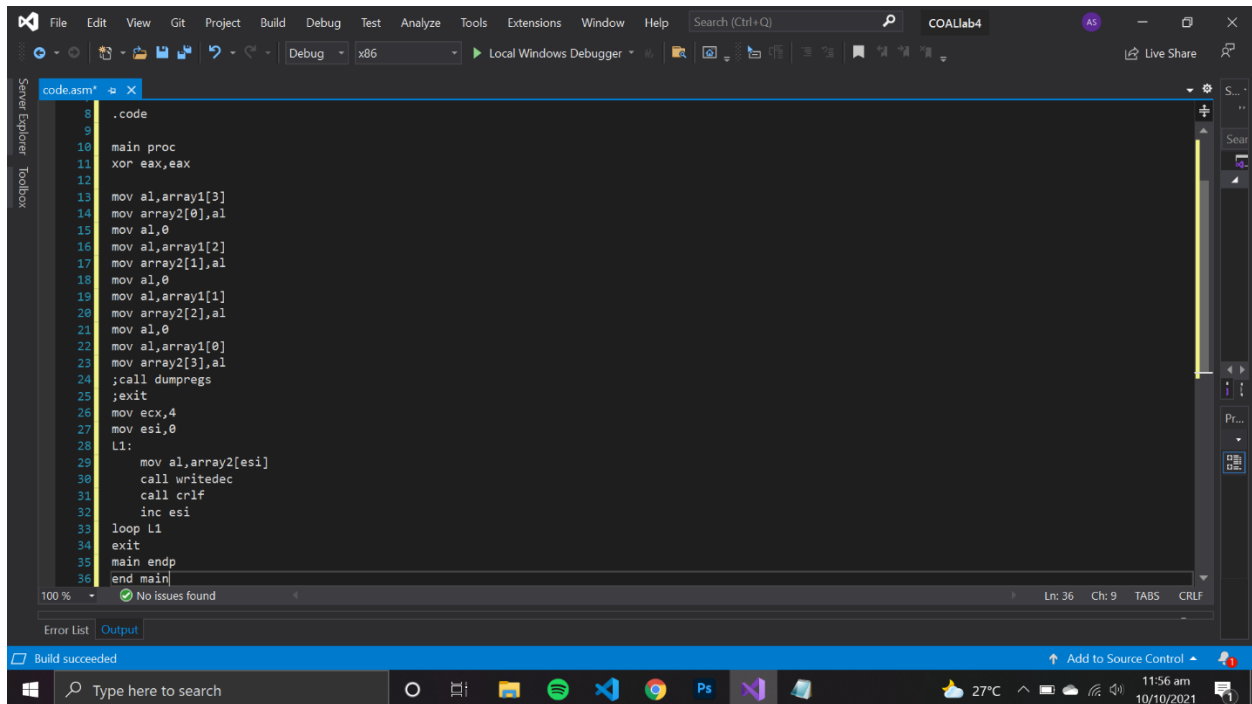


The screenshot shows the Visual Studio IDE with the 'Debug' window open. The window title is 'Select Microsoft Visual Studio Debug Console'. The output text is as follows:

```
EAX=000000FC EBX=01089000 ECX=00B110AA EDX=00B110AA  
ESI=00B110AA EDI=00B110AA EBP=0133F84C ESP=0133F840  
EIP=00B136B0 EFL=00000206 CF=0 SF=0 ZF=0 OF=0 AF=0 PF=1  
  
C:\Users\pd\source\repos\COALLab4\Debug\COALLab4.exe (process 11600) exited with code 0.  
Press any key to close this window . . .
```

The status bar at the bottom indicates 'Build succeeded' and 'No issues found'. The taskbar at the bottom shows the system clock as 11:57 am on 10/10/2021.

TASK 5:

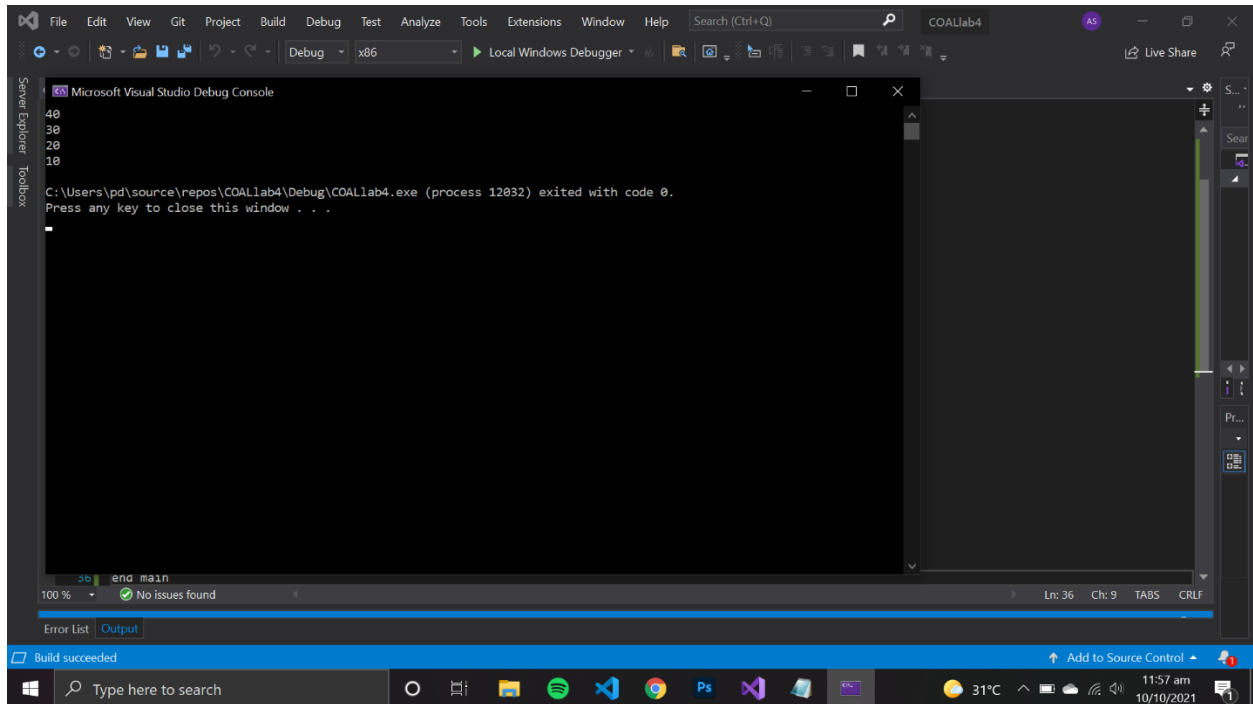


The screenshot shows the Visual Studio IDE with the 'code.asm' file open. The assembly code is as follows:

```
.code  
main proc  
xor eax,eax  
mov al,array1[3]  
mov array2[0],al  
mov al,0  
mov al,array1[2]  
mov array2[1],al  
mov al,0  
mov al,array1[1]  
mov array2[2],al  
mov al,0  
mov al,array1[0]  
mov array2[3],al  
;call dumpregs  
;exit  
mov ecx,4  
mov esi,0  
L1:  
mov al,array2[esi]  
call writedec  
call crlf  
inc esi  
loop L1  
exit  
main endp  
end main
```

The status bar at the bottom indicates 'Build succeeded' and 'No issues found'. The taskbar at the bottom shows the system clock as 11:56 am on 10/10/2021.

OUTPUT:

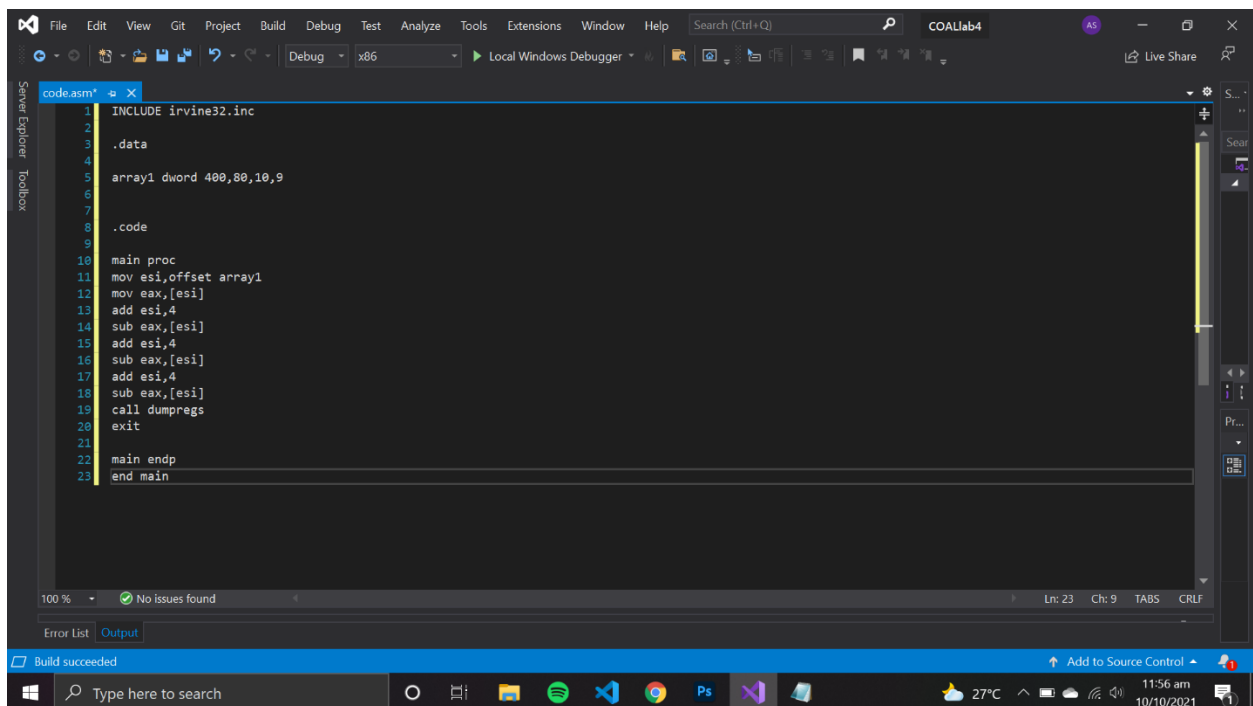


The screenshot shows the Visual Studio interface with the 'Microsoft Visual Studio Debug Console' window open. The console displays the following output:

```
40  
30  
20  
10  
  
C:\Users\pd\source\repos\COALLab4\Debug\COALLab4.exe (process 12832) exited with code 0.  
Press any key to close this window . . .
```

The status bar at the bottom indicates 'Build succeeded' and 'No issues found'. The taskbar shows the system clock as 11:57 am on 10/10/2021.

TASK 6:

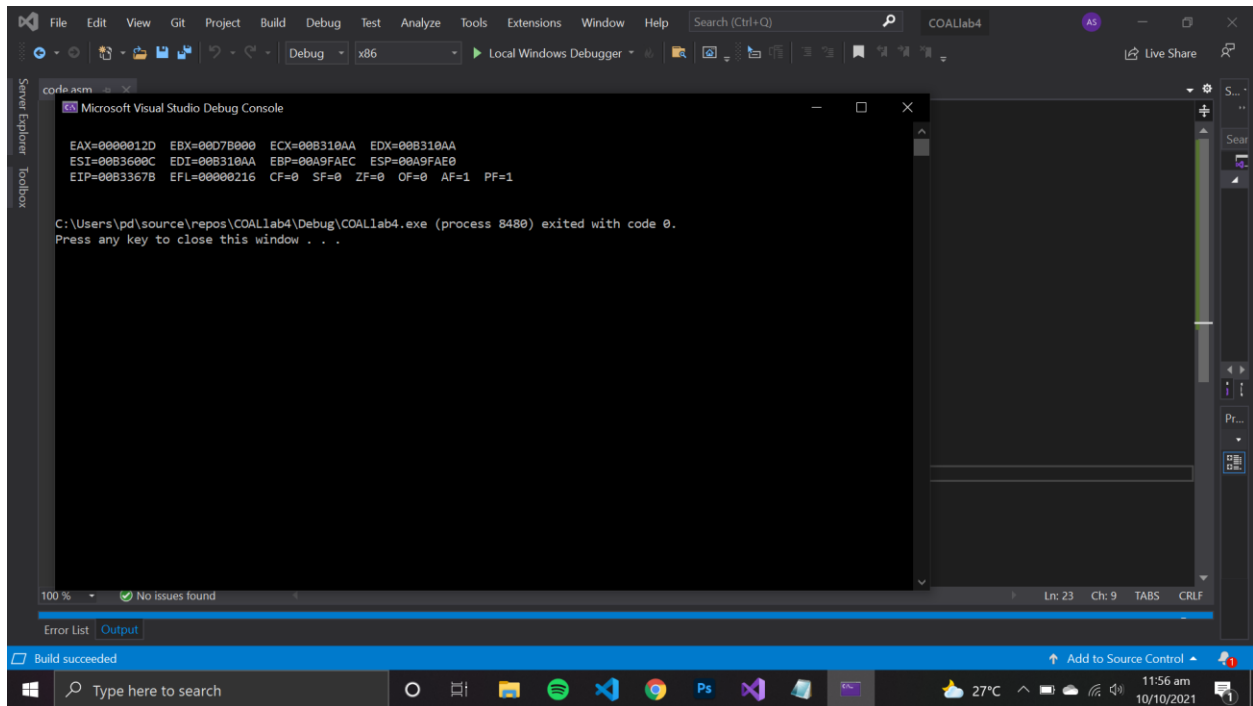


The screenshot shows the Visual Studio interface with the 'code.asm' file open in the editor. The assembly code is as follows:

```
1 INCLUDE irvine32.inc  
2  
3 .data  
4  
5 array1 dword 400,80,10,9  
6  
7  
8 .code  
9  
10 main proc  
11 mov esi,offset array1  
12 mov eax,[esi]  
13 add esi,4  
14 sub eax,[esi]  
15 add esi,4  
16 sub eax,[esi]  
17 add esi,4  
18 sub eax,[esi]  
19 call dumpregs  
20 exit  
21  
22 main endp  
23 end main
```

The status bar at the bottom indicates 'Build succeeded' and 'No issues found'. The taskbar shows the system clock as 11:56 am on 10/10/2021.

OUTPUT:

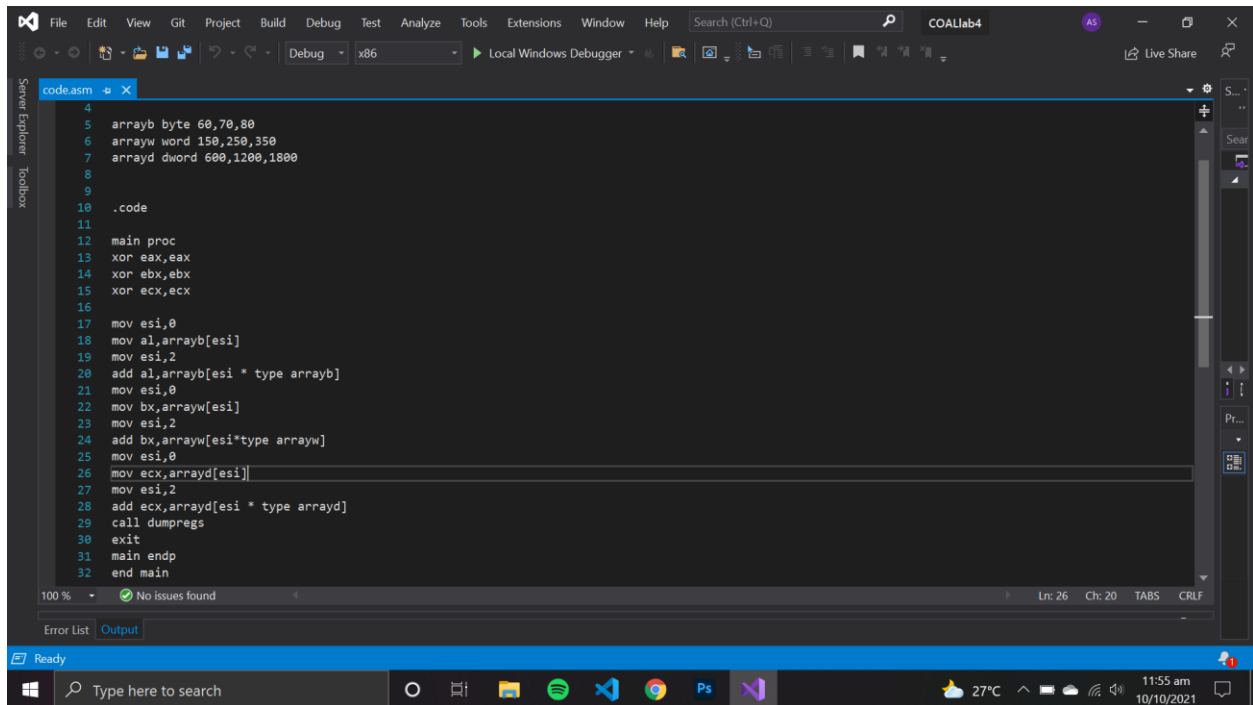


The screenshot shows the Visual Studio IDE with the 'Microsoft Visual Studio Debug Console' window open. The console displays the following output:

```
EAX=0000012D EBX=0007B000 ECX=000310AA EDX=000310AA  
ESI=0003600C EDI=000310AA EBP=00A9FAEC ESP=00A9FAE0  
EIP=00033678 EFL=00000216 CF=0 SF=0 ZF=0 OF=0 AF=1 PF=1  
  
C:\Users\pd\source\repos\COALLab4\Debug\COALLab4.exe (process 8480) exited with code 0.  
Press any key to close this window . . .
```

The status bar at the bottom indicates 'Build succeeded' and 'No issues found'. The taskbar at the bottom shows the system clock as 11:56 am on 10/10/2021.

TASK 7:

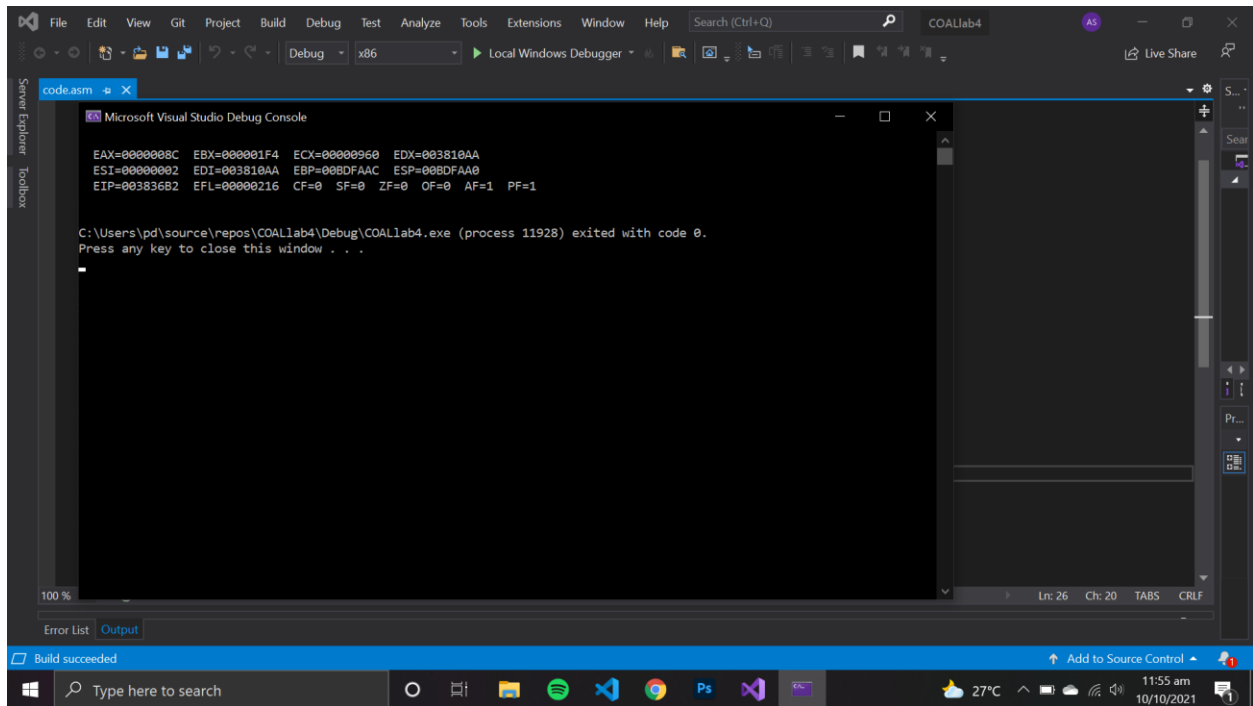


The screenshot shows the Visual Studio IDE with the 'code.asm' file open in the editor. The assembly code is as follows:

```
4  
5 arrayb byte 60,70,80  
6 arrayw word 150,250,350  
7 arrayd dword 600,1200,1800  
8  
9  
10 .code  
11  
12 main proc  
13 xor eax,eax  
14 xor ebx,ebx  
15 xor ecx,ecx  
16  
17 mov esi,0  
18 mov al,arrayb[esi]  
19 mov esi,2  
20 add al,arrayb[esi * type arrayb]  
21 mov esi,0  
22 mov bx,arrayw[esi]  
23 mov esi,2  
24 add bx,arrayw[esi*type arrayw]  
25 mov esi,0  
26 mov ecx,arrayd[esi]  
27 mov esi,2  
28 add ecx,arrayd[esi * type arrayd]  
29 call dumpregs  
30 exit  
31 main endp  
32 end main
```

The status bar at the bottom indicates 'Ready' and 'No issues found'. The taskbar at the bottom shows the system clock as 11:55 am on 10/10/2021.

OUTPUT:



```
code.asm x
Microsoft Visual Studio Debug Console

EAX=0000008C EBX=000001F4 ECX=00000960 EDX=003810AA
ESI=00000002 EDI=003810AA EBP=00BDFAAC ESP=00BDFAA0
EIP=003836B2 EFL=00000216 CF=0 SF=0 ZF=0 OF=0 AF=1 PF=1

C:\Users\pd\source\repos\COALLab4\Debug\COALLab4.exe (process 11928) exited with code 0.
Press any key to close this window . . .
```

Build succeeded

Type here to search

27°C 11:55 am 10/10/2021