



Архітектура комп'ютера

Лекція 10

Лектор:

доцент кафедри КІ та КБ,
к.т.н. Шелуха Олексій

Зміст лекції

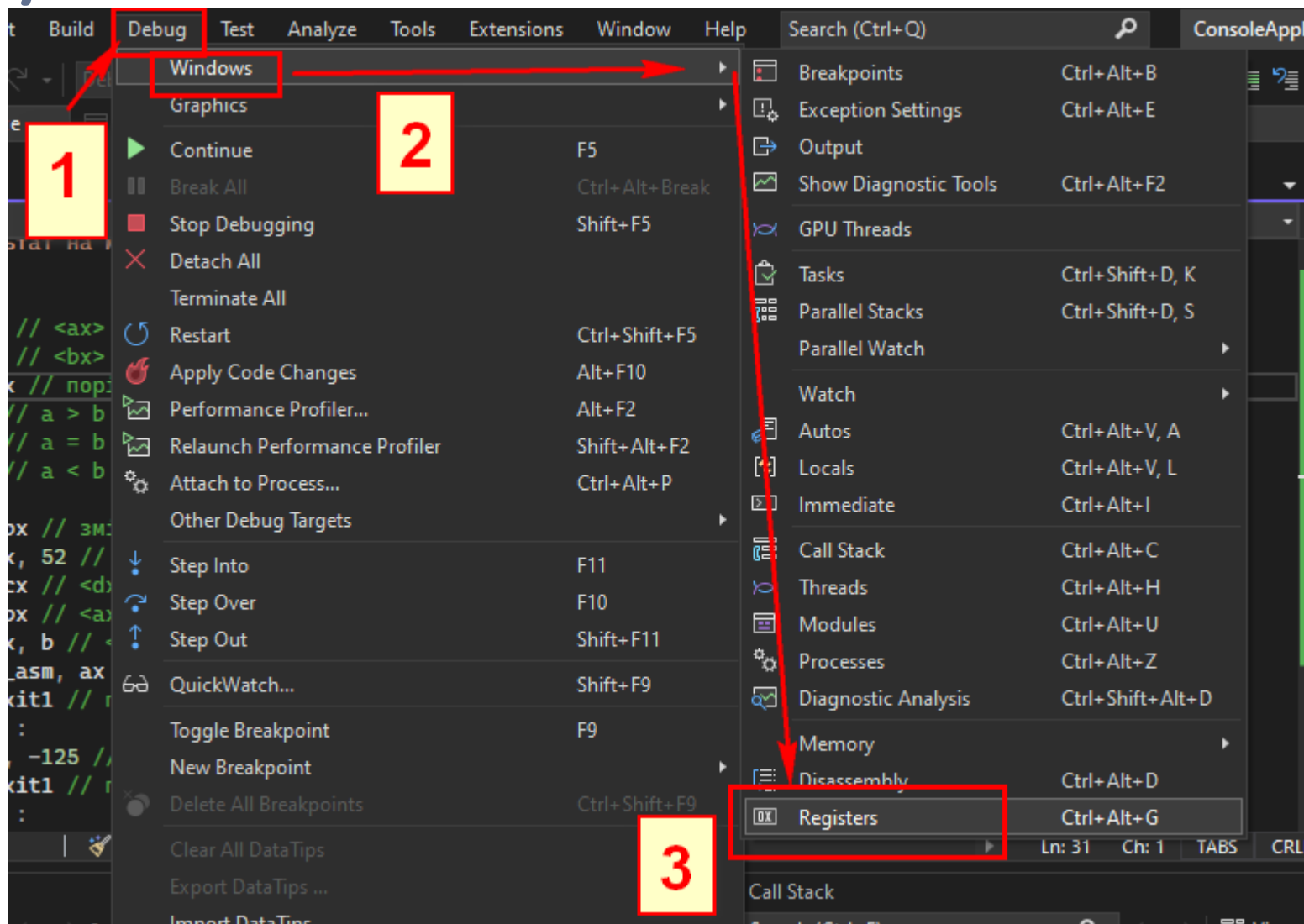
- 1. Регістри стану FLAGS/EFLAGS/RFLAGS
- 2. Відображення у Visual Studio
- 3. Аналіз прапорців
- 4. Взаємодія з прапорцями у коді

Регістри стану FLAGS/EFLAGS/RFLAGS

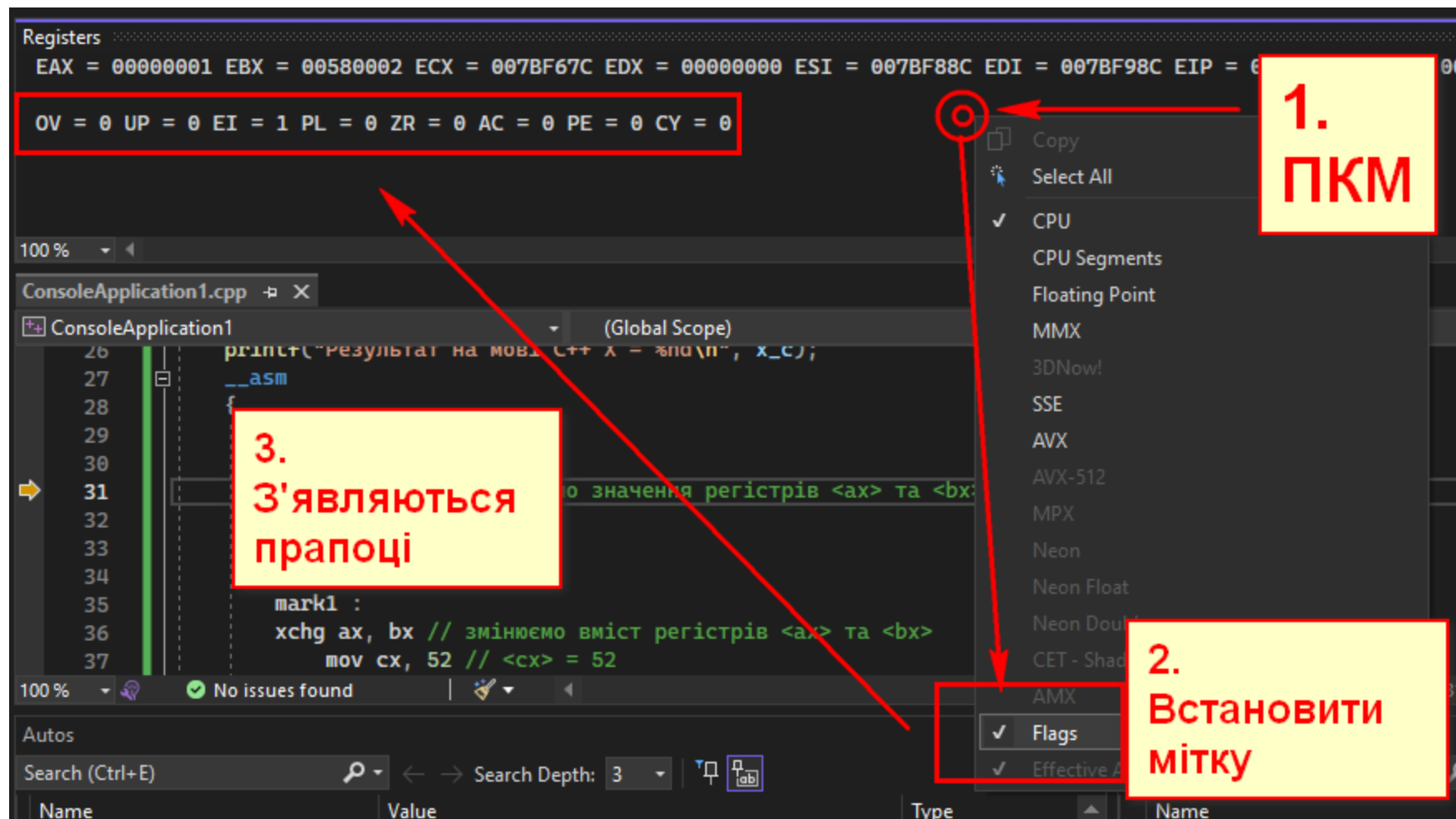
- Регістр FLAGS — це регістр стану, який містить поточний стан ЦП x86.
- Розмір і значення бітів прапора залежать від архітектури. Зазвичай він відображає результат арифметичних операцій, а також інформацію про обмеження, накладені на роботу центрального процесора в поточний момент часу. Деякі з цих обмежень можуть включати заборону запуску деяких переривань, заборону виконання класу "привілейованих" інструкцій.
- Додаткові прапорці стану можуть обходити відображення пам'яті та визначати, яку дію ЦП має виконувати у разі арифметичного переповнення.

Відображення у Visual Studio

- Під час режиму дебагінгу (F10) виконати наступні дії:
- 1. Відкрити вкладку Debug
- 2. Відкрити підвкладку Windows
- 3. Обрати пункт Registers. Або спробувати гарячі клавіші Ctrl+Alt+G (можуть відрізнятись в залежності від версії VS).

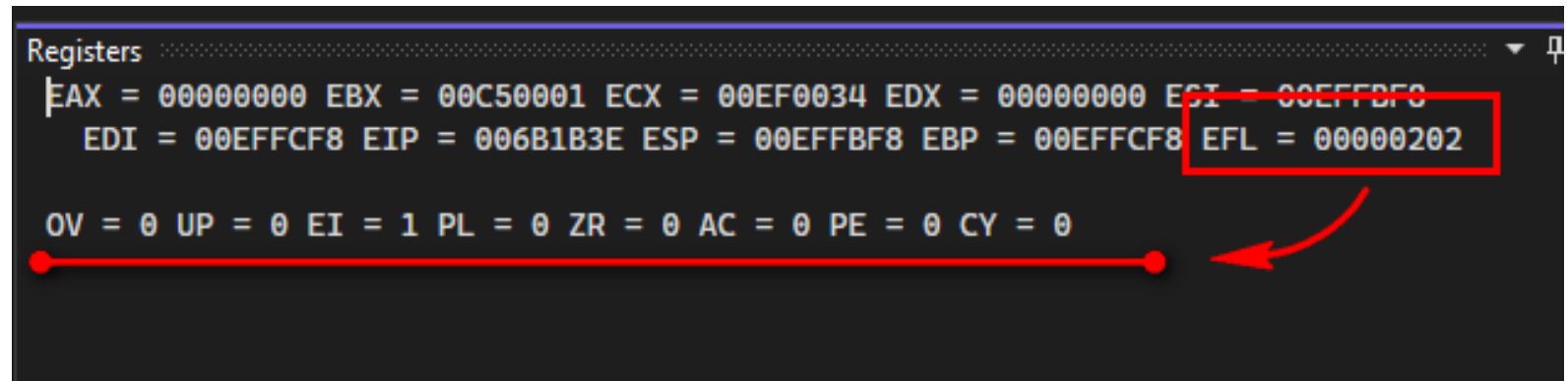


Відображення у Visual Studio



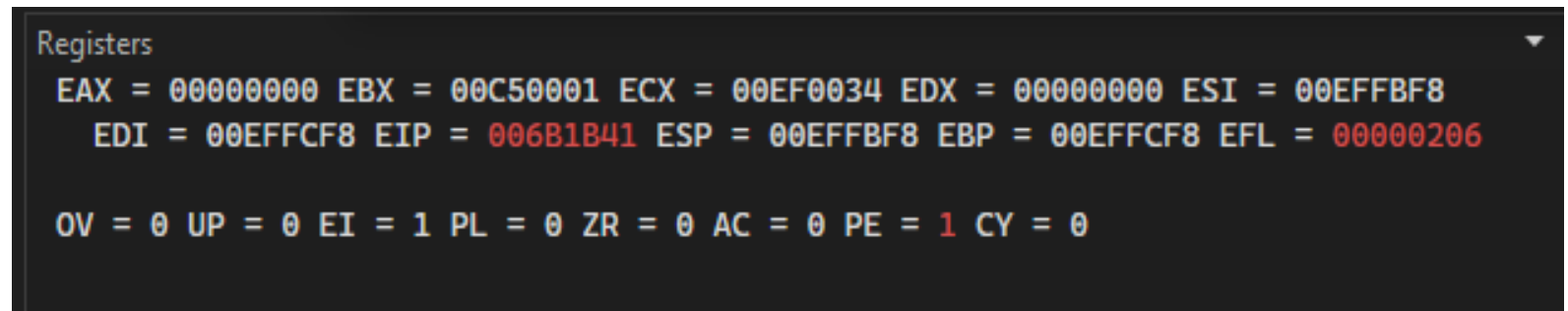
Відображення у Visual Studio

- 202h → 0010 0000 0010b
- 206h → 0010 0000 0110b



```
Registers
EAX = 00000000 EBX = 00C50001 ECX = 00EF0034 EDX = 00000000 ESI = 00EFFBF8
EDI = 00EFFCF8 EIP = 006B1B3E ESP = 00EFFBF8 EBP = 00EFFCF8 EFL = 00000202

OV = 0 UP = 0 EI = 1 PL = 0 ZR = 0 AC = 0 PE = 0 CY = 0
```



```
Registers
EAX = 00000000 EBX = 00C50001 ECX = 00EF0034 EDX = 00000000 ESI = 00EFFBF8
EDI = 00EFFCF8 EIP = 006B1B41 ESP = 00EFFBF8 EBP = 00EFFCF8 EFL = 00000206

OV = 0 UP = 0 EI = 1 PL = 0 ZR = 0 AC = 0 PE = 1 CY = 0
```

EIP1 6B1B3Eh = 0110 1011 0001 1011 0011 1110b

14 «одинчик» - парна кількість (останній байт 5 одиниць)

EIP2 6B1B41h = 0110 1011 0001 1011 0100 0001b

11 «одинчик» - непарна кількість (останній байт 2 одиниці)

Аналіз прапорців

Intel x86 FLAGS register

Bit #	Mask	Abbreviation	Description	Category	=1	=0
FLAGS						
0	0x0001	CF	Carry flag	Status	CY(Carry)	NC(No Carry)
1	0x0002	—	Reserved, always 1 in EFLAGS	—		
2	0x0004	PF	Parity flag	Status	PE(Parity Even)	PO(Parity Odd)
3	0x0008	—	Reserved	—		
4	0x0010	AF	Auxiliary Carry flag	Status	AC(Auxiliary Carry)	NA(No Auxiliary Carry)
5	0x0020	—	Reserved	—		
6	0x0040	ZF	Zero flag	Status	ZR(Zero)	NZ(Not Zero)
7	0x0080	SF	Sign flag	Status	NG(Negative)	PL(Positive)
8	0x0100	TF	Trap flag (single step)	Control		
9	0x0200	IF	Interrupt enable flag	Control	EI(Enable Interrupt)	DI(Disable Interrupt)
10	0x0400	DF	Direction flag	Control	DN(Down)	UP(Up)
11	0x0800	OF	Overflow flag	Status	OV(Overflow)	NV(Not Overflow)
12-13	0x3000	IOPL	I/O privilege level (286+ only), always all-1s on 8086 and 186	System		

Аналіз прапорців

Intel x86 FLAGS register

Bit #	Mask	Abbr.	Description	Category	=1	=0
FLAGS						
14	0x4000	NT	Nested task flag (286+ only), always 1 on 8086 and 186	System		
15	0x8000	MD	Mode flag (NEC V-series only), reserved on all Intel CPUs. Always 1 on 8086/186, 0 on 286 and later.	Control		
EFLAGS						
16	0x0001 0000	RF	Resume flag (386+ only)	System		
17	0x0002 0000	VM	Virtual 8086 mode flag (386+ only)	System		
18	0x0004 0000	AC	Alignment Check (486+, ring 3), SMAP Access Check (Broadwell+, ring 0-2)	System		
19	0x0008 0000	VIF	Virtual interrupt flag (Pentium+)	System		
20	0x0010 0000	VIP	Virtual interrupt pending (Pentium+)	System		
21	0x0020 0000	ID	Able to use CPUID instruction (Pentium+)	System		
22-31	0x3FC0 0000	—	Reserved	—		
RFLAGS						
32-63	0xFFFF FFFF... ...0000 0000	—	Reserved	—		

Приклад

- $|x| = \begin{cases} a * b, \text{ якщо } a > b \\ \frac{1}{a*(b-1)}, \text{ якщо } a \leq b \end{cases}$
- При $a, b - 8$ біт, $x - 32$ біт.

Дякую за увагу!