1 №9

1.1 :

1.1.1

1.2

1 1 2 1 3 2 4 3 4.1
NASM 3 4.2 GDB 5 4.2.1 9 4.2.2
GDB 9 4.2.3 GDB 13 4.3
15 5 21 6 21 ## 1
. GDB .
2 1. NASM. 2. GDB. 3.
. 4. GDB. 5. GDB. 6.
. ## 3 — .
, .
. —
. GDB (GNU Debugger — GNU)
UNIX- . GDB
.
. GDB
, ,
. GDB ( ) , « »
. run (r) —
GDB. kill (k) ,
. y (« »), .
run , (breakpoints), (watchpoints)
(catchpoints) . quit (q).
, ,
, .
, -g.
break (b). — .
. , « ».
info (i). - ,
disable. enable.
, delete.
continue (c). .
N, N − 1
(N-). stepi (sI) , . .
. — , , ,
.
, . ,
, . ,
.
call, eip ,
. , , ,

. ret, ,
call, eip.
, call. ## 4 ### 4.1 NASM
№ 9, lab09-1.asm. (.4.1)

```
emshekhavcov@emshekhavcov:~$ mkdir ~/work/study/2023-2024/Архитектура\ компьютера/arch-pc/lab09
emshekhavcov@emshekhavcov:~$ cd work/study/2023-2024/Архитектура\ компьютера/arch-pc/lab09
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ touch lab09-1.asm
```

lab09-1.asm 9.1. (.4.2)

Открыть

lab09-1.asm
~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09

```
%include 'in_out.asm'
SECTION .data
msg: DB 'Введите x: ',0
result: DB '2x+7=',0
SECTION .bss
x: RESB 80
res: RESB 80
SECTION .text
GLOBAL _start
_start:
;-------------------------------------
; Основная программа
;-------------------------------------
mov eax, msg
call sprint
mov ecx, x
mov edx, 80
call sread
mov eax,x
call atoi
```

```
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ nasm -f elf lab09-1.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ld -m elf_i386 -o lab09-1 lab
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ./lab09-1
Введите x: 7
2x+7=21
```

. (.4.3)
, _subcalcul _calcul
f(g(x)), x , $f(x) = 2x + 7$, $g(x) = 3x - 1$. (.4.4)

```
;---------------------------------------
; Подпрограмма вычисления
; выражения "2x+7"
_calcul:
mov ebx,2
mul ebx
add eax,7
mov [res],eax
ret ; выход из подпрограммы

_subcalcul:
mov ebx,3
mul ebx
add eax,-1
ret
```

4.2

GDB lab09-2.asm 9.2. (.4.6)

```
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ nasm -f elf lab09-1.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ld -m elf_i386 -o lab09-1 lab09-1.o
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ./lab09-1
Введите x: 7
2x+7=47
```

GDB '-g'. (.4.7)

```
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ touch lab09-2.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ nasm -f elf -g -l
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ld -m elf_i386 -o
```

gdb. (.4.8)

```
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ gdb lab
GNU gdb (Debian 13.1-3) 13.1
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab09-2...
(gdb)
```

, GDB run. (.4.9)

```
(gdb) run
Starting program: /home/emshekhavcov/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09/lab09-2
Hello, world!
[Inferior 1 (process 4110) exited normally]
(gdb)
```

_start . (.4.10)

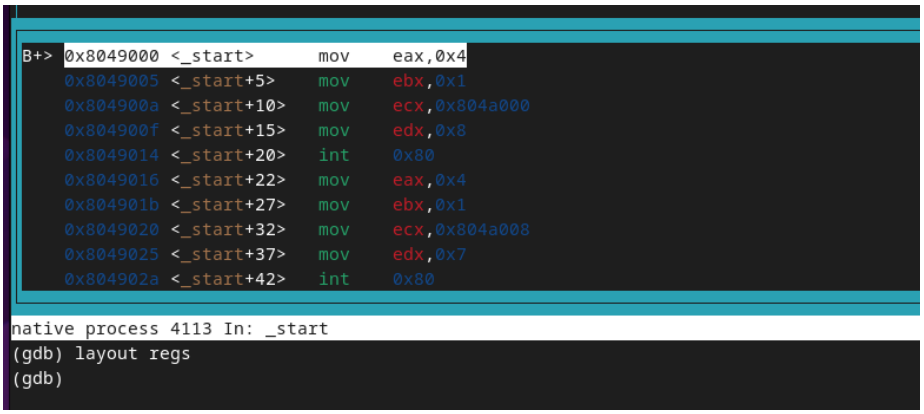
```
(gdb) break _start
Breakpoint 1 at 0x8049000: file lab09-2.asm, line 9.
(gdb) run
Starting program: /home/emshekhavcov/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09/lab09-2

Breakpoint 1, _start () at lab09-2.asm:9
9       mov eax, 4
(gdb)
```

disassemble, _start, Intel, set disassembly-flavor intel.

```
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:     mov    $0x4,%eax
   0x08049005 <+5>:     mov    $0x1,%ebx
   0x0804900a <+10>:    mov    $0x804a000,%ecx
   0x0804900f <+15>:    mov    $0x8,%edx
   0x08049014 <+20>:    int    $0x80
   0x08049016 <+22>:    mov    $0x4,%eax
   0x0804901b <+27>:    mov    $0x1,%ebx
   0x08049020 <+32>:    mov    $0x804a008,%ecx
   0x08049025 <+37>:    mov    $0x7,%edx
   0x0804902a <+42>:    int    $0x80
   0x0804902c <+44>:    mov    $0x1,%eax
   0x08049031 <+49>:    mov    $0x0,%ebx
   0x08049036 <+54>:    int    $0x80
End of assembler dump.
(gdb) set disassembly-flavor intel
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:     mov    eax,0x4
   0x08049005 <+5>:     mov    ebx,0x1
   0x0804900a <+10>:    mov    ecx,0x804a000
   0x0804900f <+15>:    mov    edx,0x8
   0x08049014 <+20>:    int    0x80
   0x08049016 <+22>:    mov    eax,0x4
   0x0804901b <+27>:    mov    ebx,0x1
   0x08049020 <+32>:    mov    ecx,0x804a008
   0x08049025 <+37>:    mov    edx,0x7
   0x0804902a <+42>:    int    0x80
   0x0804902c <+44>:    mov    eax,0x1
   0x08049031 <+49>:    mov    ebx,0x0
   0x08049036 <+54>:    int    0x80
End of assembler dump.
```

(.4.11) ATT %, $, Intel . layout asm layout regs.



(.4.12)

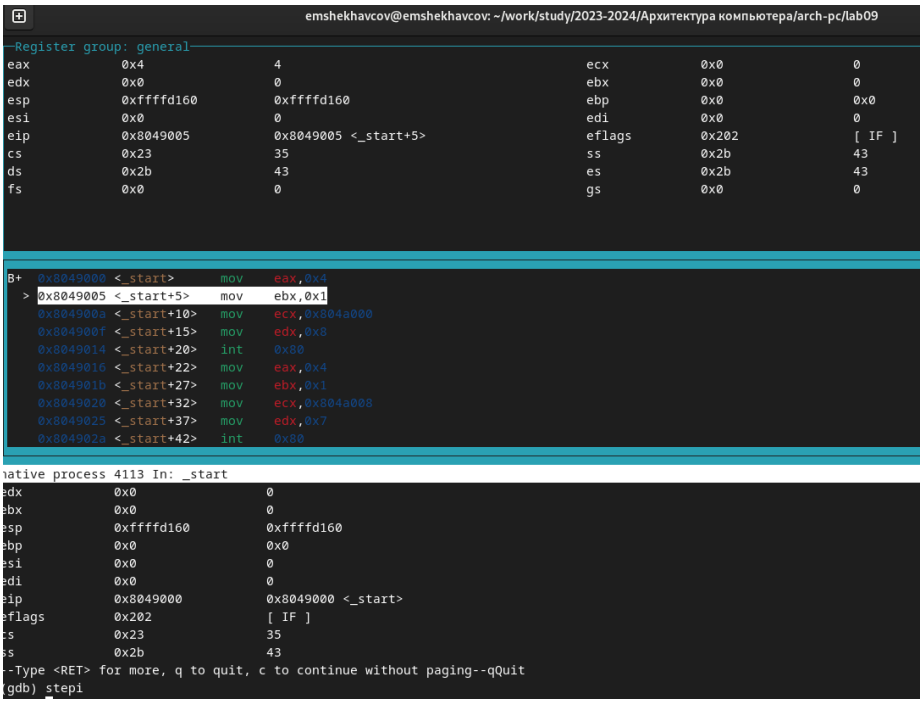
4.2.1 , _start

info breakpoints

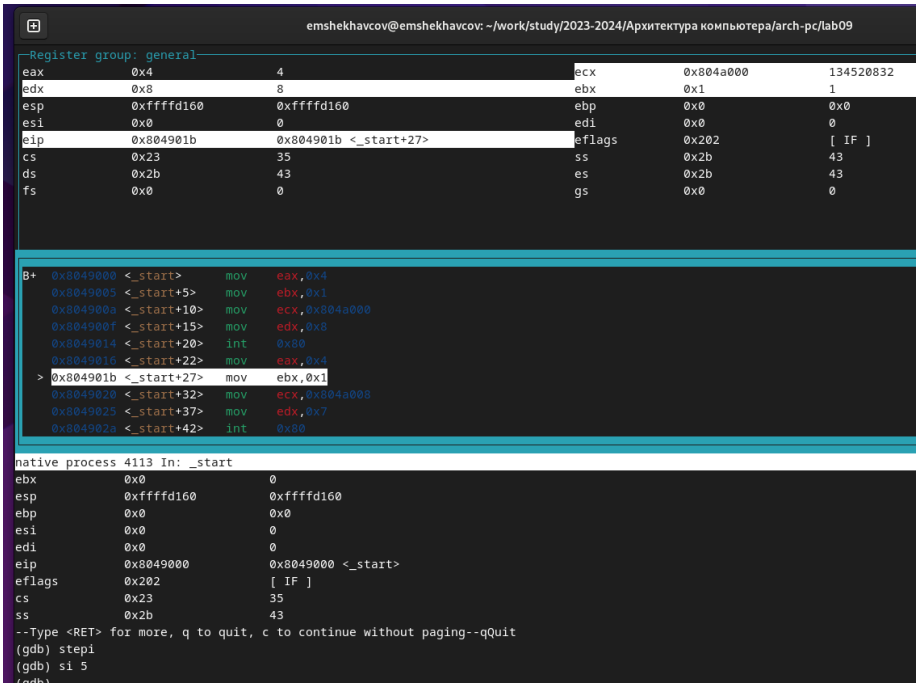
mov ebx,0x0. . (.4.13)

```
Num     Type           Disp Enb Address    What
1       breakpoint     keep y   0x08049000 lab09-2.asm:9
        breakpoint already hit 1 time
(gdb) b *0x8049031
Breakpoint 2 at 0x8049031: file lab09-2.asm, line 20.
(gdb) i b
Num     Type           Disp Enb Address    What
1       breakpoint     keep y   0x08049000 lab09-2.asm:9
        breakpoint already hit 1 time
2       breakpoint     keep y   0x08049031 lab09-2.asm:20
(gdb)
```

4.2.2 GDB 5 stepi

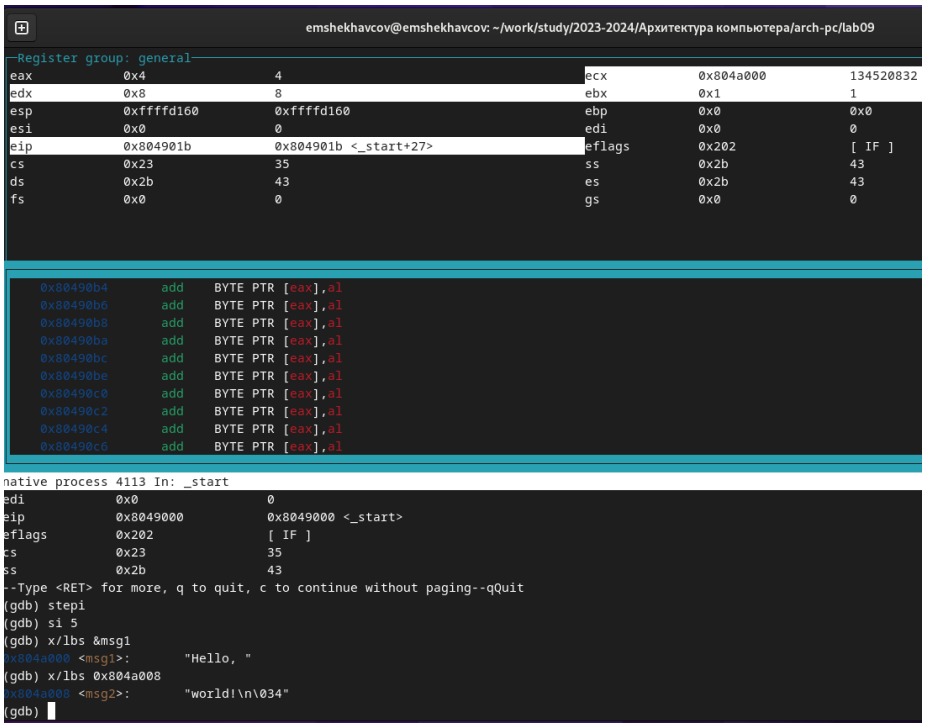


. (.4.14)



stepi.(.4.15)

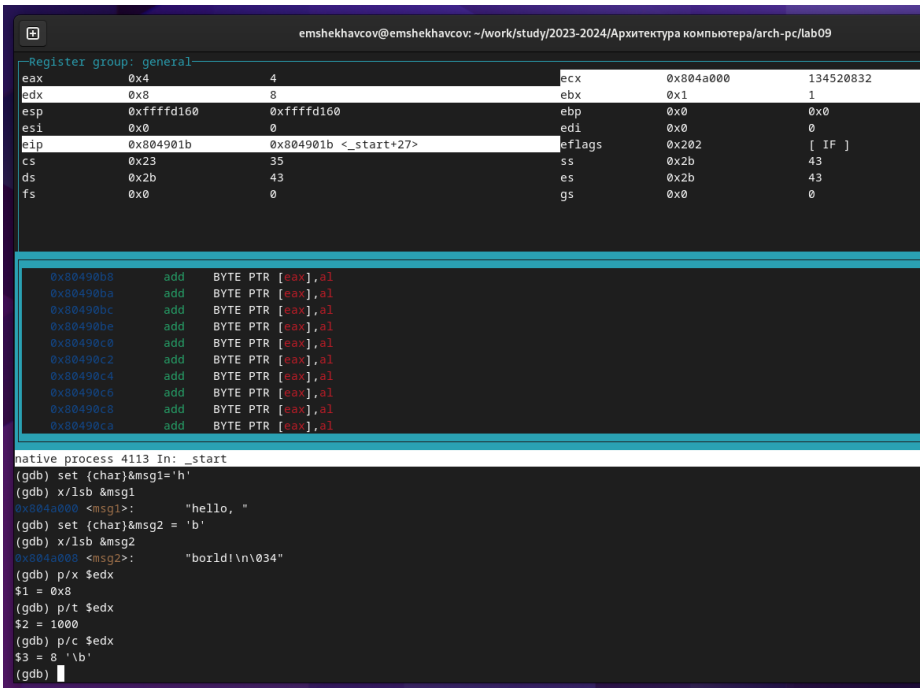
eax, ecx, edx ebx. msg1
x/1sb &msg1 msg2 . (.4.16)



set msg1 msg2.

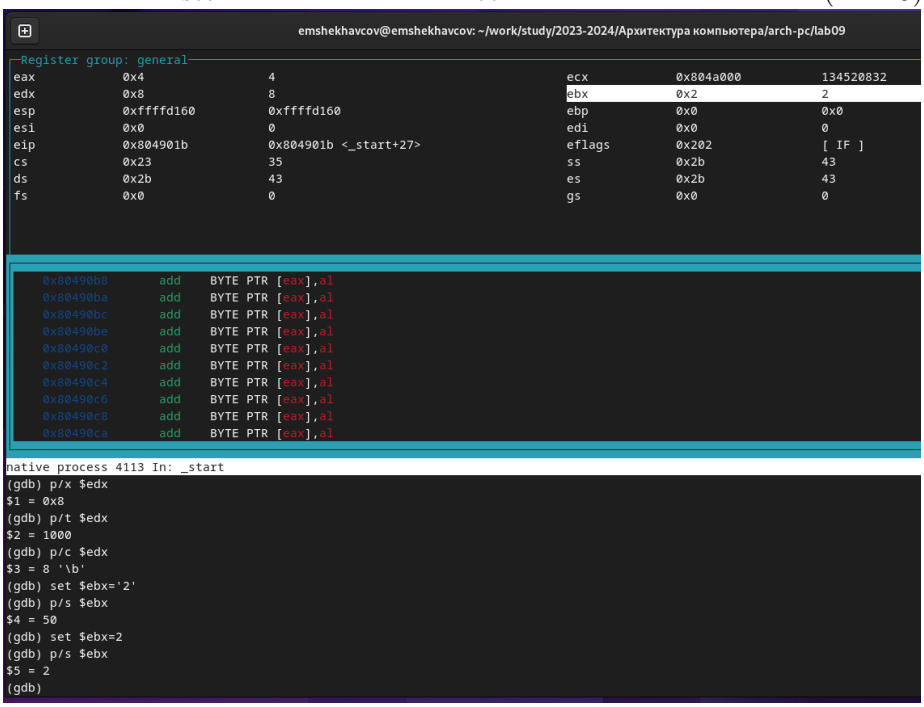
(.4.17)

, edx print p/F $val.



(.4.18)

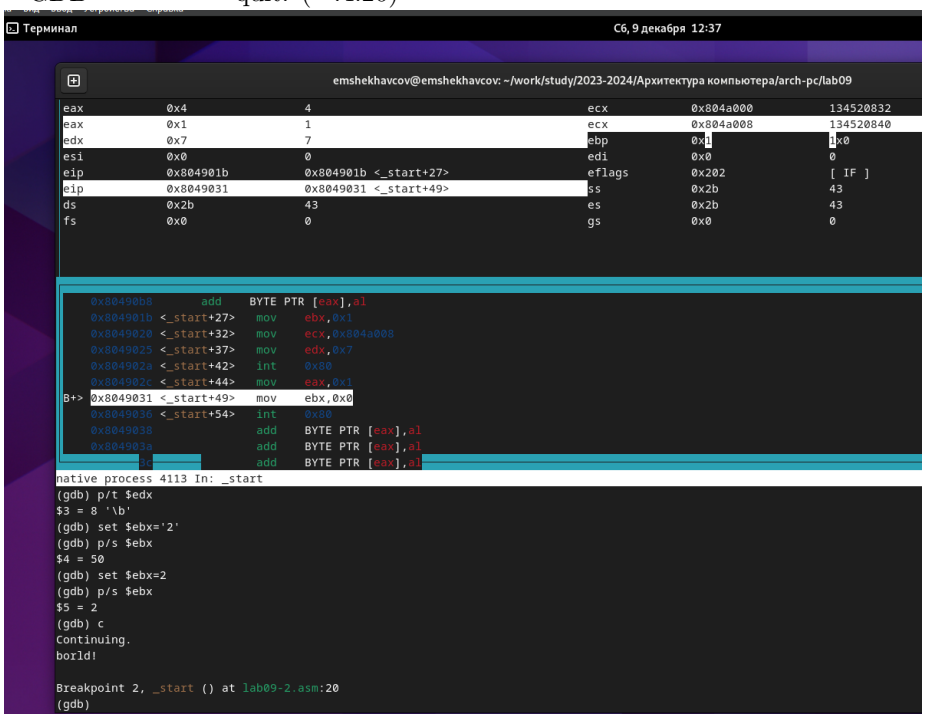
set ebx . (.4.19)



p/s $ebx , ,

. continue

GDB quit. (.4.20)



4.2.3 GDB lab8-2.asm

8.2 lab09-3.asm . (.4.21)

```
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab08$ cp ~/work/study/2023-2024/Архитектура\ компьютера/arch-pc/lab08/lab8-2.asm ~/work/study/2023-
024/Архитектура\ компьютера/arch-pc/lab09/lab09-3.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ nasm -f elf -g -l lab09-3.lst lab09-3.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ld -m elf_i386 -o lab09-3 lab09-3.o
```

gdb, –args. (.4.22)

```
emshekhavcov@emshekhavcov: ~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ gdb --args lab09-3 аргумент1 аргумент 2 'аргумент 3'
GNU gdb (Debian 13.1-3) 13.1
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab09-3...
```

. (.4.23)

```
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab09-3.asm, line 5.
(gdb) run
Starting program: /home/emshekhavcov/work/study/2023-2024/Архитектура компьютера/arch-pc/la

Breakpoint 1, _start () at lab09-3.asm:5
5       pop ecx ; Извлекаем из стека в `ecx` количество
(gdb)
```

```
(gdb) x/x $esp
0xffffd110:     0x00000005
(gdb) x/s *(void**)($esp + 4)
0xffffd2be:     "/home/emshekhavcov/work/study/2023-2024/Архитектура компьютера/arch-p
(gdb) x/s *(void**)($esp + 8)
0xffffd328:     "аргумент1"
(gdb) x/s *(void**)($esp + 12)
0xffffd33a:     "аргумент"
(gdb) x/s *(void**)($esp + 16)
0xffffd34b:     "2"
(gdb) x/s *(void**)($esp + 20)
0xffffd34d:     "аргумент 3"
(gdb) x/s *(void**)($esp + 24)
0x0:    <error: Cannot access memory at address 0x0>
(gdb)
```

. (.4.24)

4, . 4. ### 4.3

1. №8 (№1

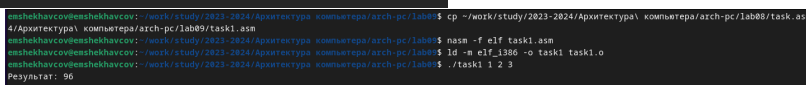
), f(x) . (.4.25)

Открыть

task1.asm

~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09

```
SECTION .text
global _start
_start:
pop ecx ; Извлекаем из стека в `ecx` количество
; аргументов (первое значение в стеке)
pop edx ; Извлекаем из стека в `edx` имя программы
; (второе значение в стеке)
sub ecx,1 ; Уменьшаем `ecx` на 1 (количество
; аргументов без названия программы)
mov esi, 0 ; Используем `esi` для хранения
; промежуточных сумм
next:
cmp ecx,0h ; проверяем, есть ли еще аргументы
jz _end ; если аргументов нет выходим из цикла
; (переход на метку `_end`)
pop eax ; иначе извлекаем следующий аргумент из стека
call atoi ; преобразуем символ в число
imul eax, 15 ; умножаем x на 15
add eax, 2 ; добавляем 2
add esi,eax ; добавляем значение функции для
; конкретного аргумента к промежуточной сумме
loop next ; переход к обработке следующего аргумента
_end:
mov eax,msg ; вывод сообщения "Результат: "
call sprint
mov eax,esi ; записываем сумму в регистр `eax`
call iprintLF ; печать результата
call quit ; завершение программы
```



, . (.4.26) : %include ‘in_out.asm’ SECTION .data msg db “ :”,0 SECTION .text global _start _start: pop ecx ; ecx ; ( ) pop edx ; edx ; ( ) sub ecx,1 ; ecx 1 (;) mov esi, 0 ; esi ; next: cmp ecx,0h ; , jz _end ; ; (_end) pop eax ; call atoi ; imul eax, 15 ; x 15 add eax, 2 ; 2 add esi,eax ; ; loop next ; _end: mov eax,msg ;

“ :” call sprint mov eax,esi ; eax call iprintLF ; call quit ; 2. task1.asm 9.3. (.4.27)

Открыть

task2.asm

~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09

```
%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
mov ebx,3
mov eax,2
add ebx,eax
mov ecx,4
mul ecx
add ebx,5
mov edi,ebx
; ---- Вывод результата на экран
mov eax,div
call sprint
mov eax,edi
call iprintLF
call quit
```

“25”. . (.4.28)

```
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ touch task2.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ nasm -f elf task2.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ld -m elf_i386 -o task2 task2.o
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ./task2
Результат: 10
```

, . GDB, , . continue . mul ecx ecx e x, 4 2, 4 5 (ebx). - , mov ecx,4 add ebx,eax mul ecx, mov eax,2. (.4.29)

```
Register group: general
eax            0x8                8
ecx            0x4                4
edx            0x0                0
ebx            0x5                5
esp            0xffffd160         0xffffd160
ebp            0x0                0x0

B+  0x80490f4 <_start+12>   mov    ecx,0x4
B+  0x80490f9 <_start+17>   mul    ecx
B+> 0x80490fb <_start+19>   add    ebx,0x5
b+  0x80490fe <_start+22>   mov    edi,ebx
    0x8049100 <_start+24>   mov    eax,0x804a000

native process 14573 In: _start
Continuing.

Breakpoint 5, _start () at task2.asm:12
(gdb) c
Continuing.

Breakpoint 6, _start () at task2.asm:13
(gdb)
```

```
Register group: general
eax            0x8                8
ecx            0x4                4
edx            0x0                0
ebx            0xa                10
esp            0xffffd160         0xffffd160
ebp            0x0                0x0

B+  0x80490f9 <_start+17>   mul    ecx
B+  0x80490fb <_start+19>   add    ebx,0x5
B+> 0x80490fe <_start+22>   mov    edi,ebx
    0x8049100 <_start+24>   mov    eax,0x804a000
    0x8049105 <_start+29>   call   0x804900f <sprint>

native process 14573 In: _start
Continuing.

Breakpoint 6, _start () at task2.asm:13
(gdb) c
Continuing.

Breakpoint 7, _start () at task2.asm:14
(gdb)
```

- . (.4.30)

, add ebx,eax mov eax,ebx ebx eax add ebx,5

Открыть task2.asm ~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09

```
%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
mov ebx,3
mov eax,2
add ebx,eax
mov eax,ebx
mov ecx,4
mul ecx
add eax,5
mov edi,eax
; ---- Вывод результата на экран
mov eax,div
call sprint
mov eax,edi
call iprintLF
call quit
```

mov edi,ebx. (.4.31)

, , ,

edx. . , . (.4.32)

```
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ nasm -f elf task2.asm
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ld -m elf_i386 -o task2 task2.o
emshekhavcov@emshekhavcov:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab09$ ./task2
Результат: 25
```

: %include ‘in_out.asm’ SECTION .data div: DB ‘ :’,0 SECTION .text GLOBAL _start _start: ; —- (3+2)*4+5 mov ebx,3 mov eax,2 add ebx,eax mov eax,ebx mov ecx,4 mul ecx add eax,5 mov edi,eax ; —- mov eax,div call sprint mov eax,edi call iprintLF call quit ## 5

GDB . ## 6

1. GDB: The GNU Project Debugger. — URL: https://www.gnu.org/software/gdb/. 2. GNU Bash Manual. — 2016. — URL: https://www.gnu.org/software/bash/manual/. 3. Midnight Commander Development Center. — 2021. — URL: https://midnight-commander. org/. 4. NASM Assembly Language Tutorials. — 2021. — URL: https://asmtutor.com/. 5. Newham C. Learning the bash Shell: Unix Shell Programming. — O’Reilly Media, 2005 — 354 . — (In a Nutshell). — ISBN 0596009658. — URL: http://www.amazon.com/Learningbash-Shell-Programming-Nutshell/dp/0596009658. 6. Robbins A. Bash Pocket Reference.

— O'Reilly Media, 2016. — 156 . — ISBN 978-1491941591. 7. The NASM documentation. — 2021. — URL: https://www.nasm.us/docs.php. 8. Zarrelli G. Mastering Bash. — Packt Publishing, 2017. — 502 . — ISBN 9781784396879. 9. . ., . . . — . : , 2018. 10. . ., . . ASSEMBLER. — . : - , 2017. 11. . . . — . : , 2016. 12. : NASM. — 2021. — URL: https://www.opennet.ru/docs/RUS/nasm/. 13. ., ., . UNIX. — 2- . — , 2010. — 656 . — ISBN 978-5-94157-538-1. 14. . NASM Unix. — 2- . — . : , 2011. — URL: http://www.stolyarov.info/books/asm_unix. 15. . . — 6- . — . : , 2013. — 874 . — (Computer Science). 16. ., . . — 4- . — . : ,2015. — 1120 . — (Computer Science).