

Universidade de Brasília
Fundamentos de Arquitetura de Computadores
Guilherme Guy de Andrade – 16/0123186
Leonardo dos Santos Silva Barreiros – 15/0135521

Trabalho 01

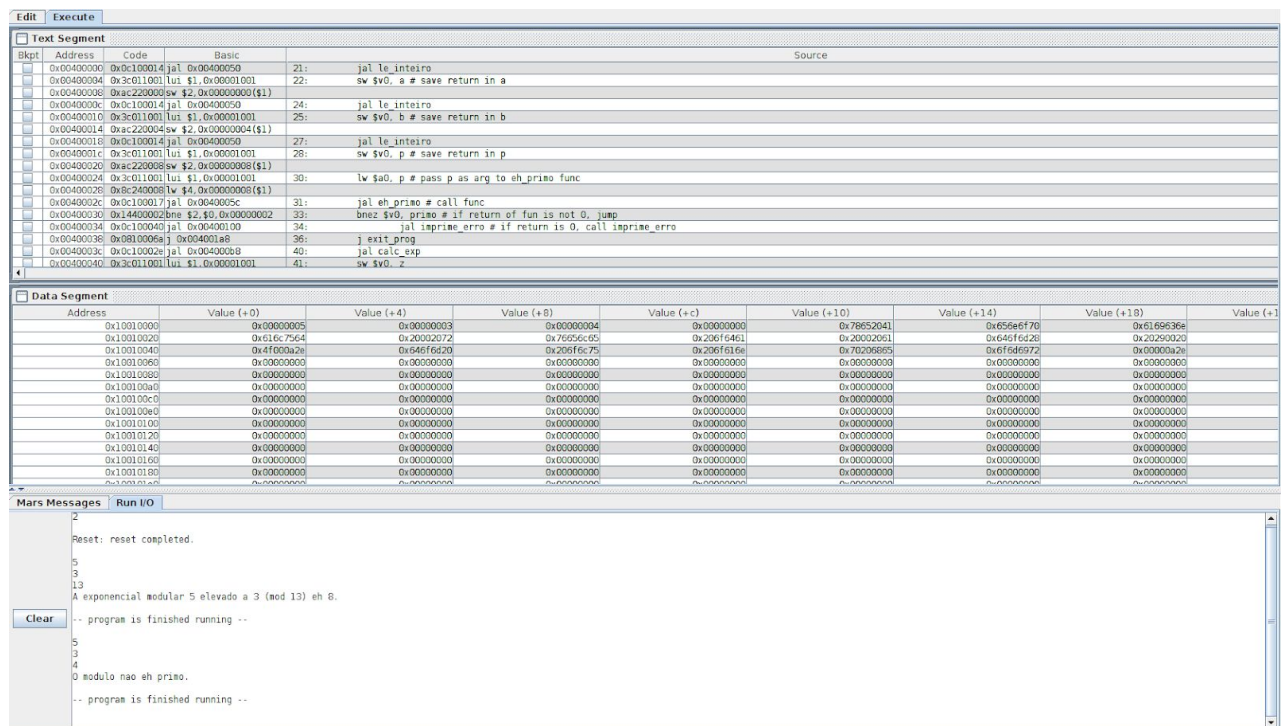
Sistema operacional foi usado na construção do sistema:

Linux Mint – 64 bits – AMD 64.

Ambiente de desenvolvimento:

MARS 4.5 – MIPS.

Instruções de Tela:



The screenshot displays the MARS MIPS simulator interface. The top section shows the assembly code with columns for EPC, Address, Code, Basic, and Source. The code includes instructions like `jal le_inteiro`, `sw $v0, a`, `sw $v0, b`, `sw $v0, p`, `lw $a0, p`, `jal eh_prime`, `bnez $v0, prime`, `jal imprime_erro`, `j exit_prog`, `jal calc_exp`, and `sw $v0, z`.

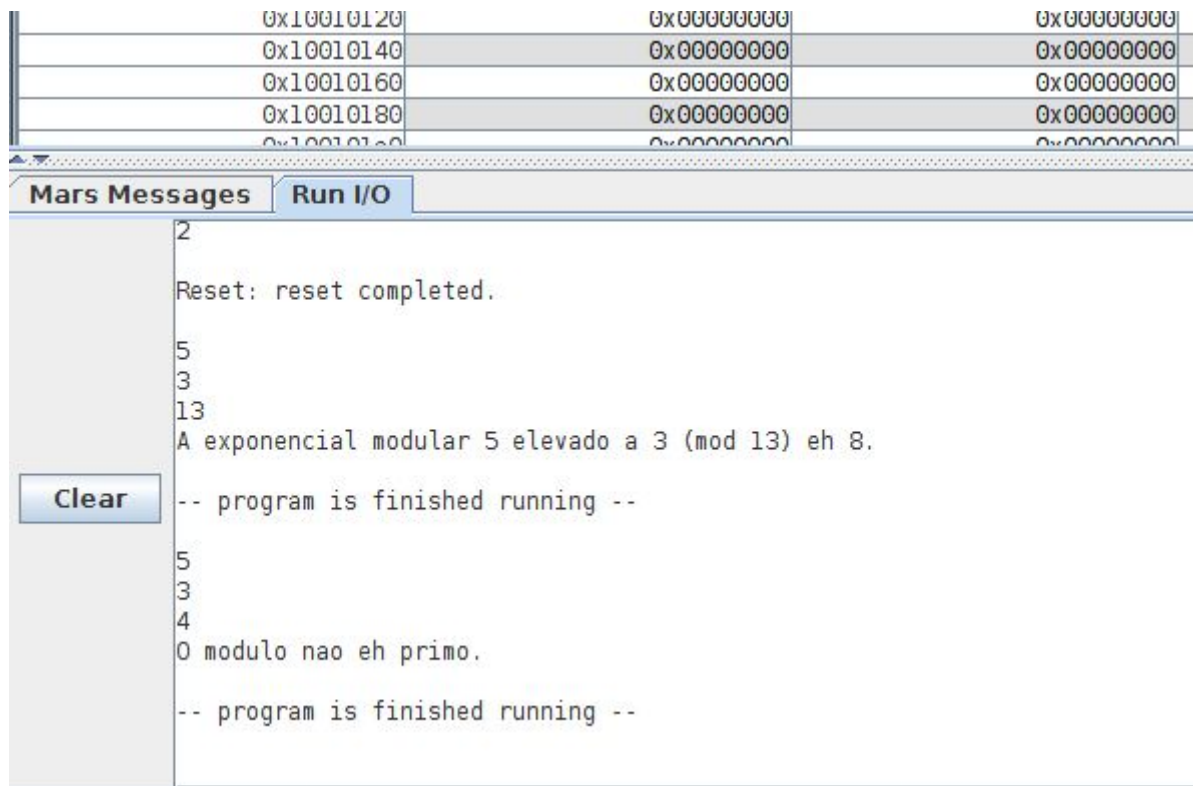
The middle section shows the Data Segment with columns for Address and Value (+0) through (+15). The values are mostly zero, except for the first few addresses which contain specific hex values.

The bottom section shows the MARS Messages window with the following output:

```

2
Reset: reset completed.
5
3
13
A exponencial modular 5 elevado a 3 (mod 13) eh 8.
Clear
-- program is finished running --
5
3
4
0 modulo nao eh primo.
-- program is finished running --

```



Após a inicialização do programa, no console do MARS, deve-se inserir na respectiva ordem:

- Um número inteiro que representa a base numérica da exponenciação;
- Um número inteiro, não negativo, que representa o expoente da operação matemática;
- Um número inteiro que será considerado como possível primo;

A inserção destes dados deve desencadear as subrotinas do programa. Caso o possível número primo que foi inserido não seja um número primo a seguinte mensagem de erro será exibida: “*O modulo nao eh primo.*”.

Caso o número for primo, será calculada a exponenciação modular com base na fórmula $[(A \wedge B) \bmod P]$, sendo A e B números inteiros e P um número primo. Após esse cálculo a seguinte mensagem será exibida no console MARS: “*A exponencial modular A elevado a B (mod P) eh Z.*”, em que A, B e P são substituídos pelos valores citados anteriormente e Z é substituído pelo valor resultante da operação matemática.

limitações conhecidas:

- O número primo opera com um valor limite de um inteiro de 16 bits;
- Lentidão no cálculo com valores elevados;
- Para números grandes o resultado não é calculado corretamente;
- Em alguns casos o resultado fica negativo;