CS 341 - Computer Architecture Lab
Assignment 3 - Assembly Language Programming

August 8, 2018

Problem 1. Modulo Arithmetic - Write an assembly language program for MIPS processor to perform the following modulo arithmetic operations:

1. Modulo addition , i.e., $(a + b) \mod n$
2. Modulo subtraction , i.e., $(a - b) \mod n$
3. Modulo multiplication , i.e., $(a * b) \mod n$
4. Modulo exponentiation , i.e., $(a^b) \mod n$
5. **(Optional)** Modulo inverse , i.e., $(a^{-1}) \mod n$
6. A variation of Discrete Logarithm , i.e., Let $b = a^x \mod n$. Given a, b and n, find minimum x.

To the extent possible, each operation should be implemented as a separate subroutine. Assume that a, b and n are each k-bit non-negative integers, k < 16 and n > 0.

Your program should present the following interface (I/O) to the user. The program should continue to run until user enters 6 to exit.

```
Enter operation code (1-add, 2-subtract, 3-multiply, 4-exponentiation,
5-inversion, 6-logarithm, 7-exit): 4
Enter a: 3
Enter b: 11
Enter n: 10
Result = 7
Enter operation code (1-add, 2-subtract, 3-multiply, 4-exponentiation,
5-inversion, 6-logarithm, 7-exit): 6
Enter a: 2
Enter b: 4
Enter n: 7
Result = 2
Enter operation code (1-add, 2-subtract, 3-multiply, 4-exponentiation,
5-inversion, 6-logarithm, 7-exit): 7
```

Note that the first line (Enter operation...exit):) is to be displayed in a single line.

Submission Guidelines

Please follow the following directory structure for submission.

```
la3_[roll-no.]
└── problem1.s
```

Compress the directory `la3_[roll-no.]` as a `.tar.gz` file and upload it on moodle.

Deadline - 5:00 PM, 8st August 2018