COMP90043: Cryptography and security: ©University of Melbourne, School of Computing and Information Systems 2020
Additional Exercises for Practice
Lecturer Udaya Parampalli

Can you answer the following questions by making use of mathematical properties that you have learned so far? Please observe the patterns, you may use the results we discussed by Euler and Fermat's theorems.

(1) Simplify the following expressions:
  (a) $64 \ (mod\ 10\ ) =$
  (b) $100003\ (\ mod\ 100) =$
  (c) $2^{145}\ 3^{777}\ 9^{777}\ (mod\ 4) =$
  (d) $4^{8}\ (mod\ 15) =;$
  (e) $3^{123}\ 5^{456}\ 7^{789}\ (mod\ 4) =$

The following results can be proved from first principles as we did with division theorems. Your task now is to verify them using magma or some small examples. Then can you think about how you can use these identities to simplify evaluation of modular expressions

(2) Verify the following identities.

$$((x\ mod\ m) + (y\ mod\ m))\ mod\ m = (x + y)\ mod\ m,$$

$$((x\ mod\ m) \times (y\ mod\ m))\ mod\ m = (x \times y)\ mod\ m,$$

where x, y and m are integers.

(3) Write an efficient algorithm for computing exponentiation in a finite structure (a group, modulo p, finite field etc).

(4) The question above is from your background on complexity theory. The objective is to show that exponentiation can be efficiently implemented. Note that the converse operation of finding discrete logarithm is not easily implementable. Nevertheless, people come up with heuristics to solve this problem.

Can you research what is the latest progress on the complexity of the discrete logarithm problem over numbers modulo a prime?

(5) Find x^5 $(mod\ 10)$, where is x is an integer and
(a.) $0 \leq x < 10$
(b.) $x \geq 10$.

(6) Express the following numbers as a product of primes and prime powers. $32, 63, 64, 79, 81, 124, 141, 234, 512$

(7) Using the results of the above question, find gcd of the following sequences of numbers.
(a) 32, 63
(b) 141, 81
(c) 81, 124
(d) 79, 141
(e) 512,81
(f) 124, 512.

(8) Set of residues modulo n, denoted by Z_n, is given by $\{0, 1, \cdots, n-1\}$.
Reduced set of residues is the set of all residues moulo n which are relatively prime to n.

How many elements are there in the reduced set of residues:
(a) modulo 11;

```
10; they are 1,2,3,4,5,6,7,8,9,10
```

(b) modulo 35;
(c) modulo 26;
(d) modulo 29;
(e) modulo 77.

In general, if a number n can be expressed using its prime factors such that $n = {p_1}^{a_1}{p_2}^{a_2}\cdots{p_n}^{a_n}$, then there are $\phi(n)$ elements in its reduced set of residues and,

$$\phi(n) = {p_1}^{a_1-1}(p_1-1){p_2}^{a_2-1}(p_2-1)\cdots{p_n}^{a_n-1}(p_n-1)$$