COMP90043 Cryptography and security: Additional Exercises: A model Solution

(1) Division Algorithm (Refer to (4.1) of the textbook).
You could use the identities:
$((x \text{ mod } m) + (y \text{ mod } m)) \text{ mod } m = (x + y) \text{ mod } m$;
$((x \text{ mod } m) * (y \text{ mod } m)) \text{ mod } m = (x * y) \text{ mod } m$;

```
You can prove the above identities by using division theorem.
For solving the problems, an appreciation and a basic
understanding are sufficient. Please try the identities
using some examples on any long integer package such as Magma.
```

Perform the following operations:
(a) $(7 - 8) \text{ mod } 11 = -1 = 10$
(b) $(2 * 4 + 7) \text{ mod } 5 = 0$
(c) $(10 * 10 - 3) \text{ mod } 11 = 9$
(d) $(1 + 2 + 3 + 4....9 + 10) \text{ mod } 11 = 0$
(e) $(1 + 2 + 4 + 8 + 16) \text{ mod } 31 = -1 = 30$

(2) Prove the following.

(a) Let a be represented as decimal number. Prove that (a mod 10) is simply ones-place in the decimal notation of a. Prove that (a mod 100) is simply the two digit number made up of the tens and ones place digits in the decimal notation of a.
Represent the number in decimal system and apply the identities given above. 10^k **mod** 10 **is** 0**.**
(b) Prove that for all positive integers n,
$2*(1+2+3+...+n) \text{ mod } (n+1) = 0$. **Use the identity:** $1 + 2 + \cdots n = n(n + 1)/2$**.**
(c) Prove that for all positive integer m,
$(1 + 2 + 4 + 8 + ... + 2^m) \text{ mod } 2^{(m+1)} = -1$.
Use the identity: $2^0 + 2^1 + \cdots 2^m = 2^{(m+1)} - 1$**.**

(3) Inverse (modulo n).

(a) By trial and error find multiplicative inverse of 43 mod 100. (How much time did you need to workout the result?). **Easy exercise- let the inverse be** y**.**

(b) Now find the inverse of 57 mod 100. 57 **is** $(100 - 43)$**, i.e** -43**, so the inverse of** 57 **is** $-y$s

(c) Draw multiplication table showing a*b mod 7 for all a,b from1 to 6.

Easy exercise, the purpose is to get a concrete example for a multiplicative group.

(d) Use the gcd algorithm to solve the following:

(i) Find gcd(23,77).

(ii) Find gcd(11,100).

(iii) Find gcd(2023,3212).

(iv) Find gcd(7,31).

(v) Find gcd(101,17).

Easy exercise.

(4) Extended GCD algorithm. Read the material about it on Page 137-139 of the textbook.

(a) Apply the extended gcd algorithm for enumerated items in the previous question.

(b) State the extended gcd algorithm.

(c) Try out xgcd algorithm on magma http://magma.maths.usyd.edu.au/magma/

(d) Write a magma function for inverse modulo n using XGCD algorithm.

(e) Try out the following exercises from Stallings textbook:

Q.4.6, Q 4.10, Q. 4.15, Q4.19 and Q 4.20

(f) Challenging probs:

try out the following exercises from Stallings textbook: Q 4.8, Q. 4.9 and Q.4.11.

(5) Factors and Divisibility:

(a) Find the factors of the following numbers: $31, 63, 2^{10} - 1, 2^{11} - 1$. **You may need to use magma or simple calculations.**

(b) Prove the Fermats theorem: For any $a < p \neq 0$, p a prime number,

$$a^{p-1} = 1 \bmod p.$$

We worked out in a workshop-Also in the text-book.

(c) How can you use the above theorem to find the inverse of a non-zero number modulo p?
We also discussed in the class, notice that $a^{p-1} = 1$ can be written as $a^{p-2}a = 1$, clearly implying a^{p-2} is the inverse of a.

(d) Eulers Totient Function: Let $\phi(n)$= number of integers less than n but relatively prime to n.

(i) Find $\phi(7)$= 6.
(ii) Find $\phi(35) = 6 \times 4 = 24$
(iii) Find $\phi(p)$ for any prime p= $p - 1$.
(iv) Find $\phi(pq)$ for any prime p and $q = (p-1)(q-1)$
(v) Prove that

$$a^{(\phi(n))} = 1 \bmod n,$$

where $a < n$ and relatively prime to n.

Euler's Theorem: We worked out in a workshop- Also in the textbook.

(6) Complexity of long integer arithmetic.
What are the complexities in big O notation for the following operations?

(a) Addition of two k-bit integers. $O(k)$.
(b) Subtraction of two k-bit integers$O(k)$.
(c) Multiplication of two k-bit integers$O(k^2)$.
(d) Division of a k-bit integer by another k-bit integer$O(k^2)$.
(e) Greatest common divisor of two k-bit integers $O(k^2)$
(f) Exponentiation a^e mod n, where a and n are k bit integers and e a m bit integerw.$O(m)$ k **bit operations**

(7) Consider some examples of polynomails over finite fields and show the workings of multiplication and division involving them.

(8) Use the irreducible polynomial $1+x^2+x^3$ in the the finite field $GF(8)$ tab

i	Elements:x^i	As Polynomials	As Vectors
$-\infty$	0	0	$[0,0,0]$
0	1	1	$[1,0,0]$
1	x	x	$[0,1,0]$
2	x^2	x^2	$[0,0,1]$
3	x^3	$1+x^2$	$[1,0,1]$
4	x^4	$1+x+x^2$	$[1,1,1]$
5	x^5	$1+x$	$[1,1,0]$
6	x^6	$x+x^2$	$[0,1,1]$
7	x^7	1	$[1,0,0]$

TABLE 1. Elements of $GF(2^3)$ as powers of x

(a) Solve $y * x^6 = 1$. $y = x$
(b) Solve $y * x^4 = x^2 .y = x^5$
(c) Compute $(x+x^2)*(x^2+x)$ **Answer** $= x^{12} = x^5 = 1+x$

(9) Consider the finite field $GF(9)$ as discussed in class last week:

i	Elements:x^i	As Polynomials	As Vectors
$-\infty$	0	0	$[0,0]$
0	1	1	$[1,0]$
1	x	x	$[0,1]$
2	x^2	$1+2*x$	$[1,2]$
3	x^3	$2+2x$	$[2,2]$
4	x^4	2	$[2,0]$
5	x^5	$2x$	$[0,2]$
6	x^6	$2+x$	$[2,1]$
7	x^7	$1+x$	$[1,1]$
8	x^8	1	$[1,0]$

TABLE 2. Elements of $GF(3^2)$ as powers of x

(a) Solve $y * x^2 = 1$.
(b) Solve $y * x^3 = x^2$.
(c) Compute $(x+1) * (x+2)$

Try these yourselves simialr to the method in the previous question.