

**COMP90043 Cryptography and security: Special Session  
on Week 10**

(1) Division Algorithm

Refer to (4.1) of the textbook.

You could use the identities:

$$((x \bmod m) + (y \bmod m)) \bmod m = (x + y) \bmod m;$$

$((x \bmod m) * (y \bmod m)) \bmod m = (x * y) \bmod m$ ; Perform the following operations:

(a)  $(7 - 8) \bmod 11 = -1 = 10$

(b)  $(2 * 4 + 7) \bmod 5 = 0$

(c)  $(10 * 10 - 3) \bmod 11 = 9$

(d)  $(1 + 2 + 3 + 4 + \dots + 9 + 10) \bmod 11 = 0$

(e)  $(1 + 2 + 4 + 8 + 16) \bmod 31 = -1 = 30$

(2) Prove the following.

- (a) Let  $a$  be represented as decimal number. Prove that  $(a \bmod 10)$  is simply ones-place in the decimal notation of  $a$ . Prove that  $(a \bmod 100)$  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.  $10^k \bmod 10$  is 0.**

- (b) Prove that for all positive integers  $n$ ,  $2 * (1 + 2 + 3 + \dots + n) \bmod (n + 1) = 0$ . **Use the identity:**  $1 + 2 + \dots + n = n(n + 1)/2$ .

- (c) Prove that for all positive integer  $m$ ,  $(1 + 2 + 4 + 8 + \dots + 2^m) \bmod (2^{m+1}) = -1$ .

**Use the identity:**  $2^0 + 2^1 + \dots + 2^m = 2^{m+1} - 1$ .

(3) Inverse (modulo  $n$ ).

- (a) By trial and error find multiplicative inverse of 43 mod 100. (How much time do you take it?). **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  $-ys$**

- (c) Draw multiplication table showing  $a*b \bmod 7$  for all  $a, b$  from 1 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)  $\gcd(11, 100)$ .
  - (iii)  $\gcd(2023, 3212)$ .
  - (iv)  $\gcd(7, 31)$ .
  - (v)  $\gcd(101, 17)$ .

**Easy exercise.**

- (4) Extended GCD algorithm. Read the material about it on Page 137-139 of the textbook.
- (a) Apply extended gcd algorithms for questions in 2.
  - (b) State 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:  $31, 63, 2^11 - 1$ .  
**You may need to use magma or simple calculations.**
- (b) Prove the Fermats theorem: For any  $a < p \neq 0$ ,  $p$  a prime number,

$$a^{(p-1)} = 1 \pmod{p}$$

.

**We worked out in a workshop-Also in the textbook.**

- (c) 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

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

**Eulers 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  $a^e \pmod{n}$ , where  $a$  and  $n$  are  $k$  bit integers and  $e$  a  $m$  bit integer.  $O(m) \cdot k$  **bit operations**
- (7) Give examples of polynomials over finite fields and illustrate multiplication and division.
- (8) Use the irreducible polynomial  $1 + x^2 + x^3$  in 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.**