الجامعة المستنصرية /كلية التربية / قسم علوم الحاسبات

4th Class
Computers & Data Security
أمنية الحاسوب والبيانات

أستاذ المادة

أ.م . د . اخلاص عباس البحراني && م.د. بيداء عبد الخالق

Chapter three
Mathematics Background

Modular Arithmetic

- several important cryptosystems make use of modular arithmetic. This is when the answer to a calculation is always in the range 0 – *m* where m is the **modulus**.
- (a mod n) means the remainder when a is divided by n.
- a mod n = r
- a div n=q
- a = qn + r
- r = a – q * n

Example :- if a=13 and n=5, find q and r.

q=13 div 5=2 and r=13-2 *5=**3** which is equivalent to (13 mod 5)

Example :- find (-13 mod 5).

This can be found by find the number (b) where 5*b >13 then let b=3 and 5*3=15 which is less than 13 so

-13 mod 5=5*3-13=**2**

- **Properties of Congruences.**
  - Two numbers a and b are said to be “congruent modulo n” if

(a mod n) = (b mod n) → $a \equiv b \pmod{n}$

- The difference between a and b will be a multiple of n So **a-b = kn** for some value of k. If and only if one of these three conditions is satisfied:-

  1. a mod n = b mod n
  2. n/(a-b) note that no remainder from this division.
  3. $a \times k + b = n$ where k is an integer.

- ***Example*** **(1) :-** $3 \equiv 2 \bmod 5$ _____ a=3 b=2 n=5
- 1. a mod n = b mod n

  3 mod 5 = 2 mod 5 $3 \neq 2$ (not satisfied)
- 2. n/(a-b)

  5/(3-2)

  5/1 = 5
- 3. $a \times k + b = n$

  $3 \times k + 2 = 5$

  3k = 5-2

  3k = 3 → k=1 (must be integer)

- ***Example*** (2) :- $17 \equiv 2 \bmod 5$ ______ a=17 b=2 n=5
- 1. a mod n = b mod n

  17 mod 5 = 2 mod 5

  2 = 2 (this condition is satisfied)
- 2. n/(a-b)

  5/(17-2)

  5/15 (not satisfied because the result is not integer number)
- 3. $a \times k + b = n$

  $17 \times k + 2 = 5$

  17k = 5-2

  17k = 3 → k=3/17 (k must be integer, not satisfied because the result is not integer number)

Examples *$4 \equiv 9 \equiv 14 \equiv 19 \equiv -1 \equiv -6 \bmod 5$,* $73 \equiv 4 (\bmod 23)$

- **Properties of Modular Arithmetic.**
  1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

- Examples

$11 \bmod 8 = 3$; $15 \bmod 8 = 7$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$

$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$

$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$

$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

- **Exponentiation** is done by repeated multiplication, as in ordinary arithmetic.
- Example

$$\textit{To find } (11^7 \bmod 13) \textit{ do the followings}$$

$$11^2 = 121 \equiv 4 (\bmod 13)$$

$$11^4 (11^2)^2 \equiv 4^2 \equiv 3 (\bmod 13)$$

$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 (\bmod 13)$$

- **Greatest Common Divisor(GCD).**
- GCD (***Greatest Common Divisor***) of two or more integers, where at least one of them is non zero, is the largest positive integer that divides the numbers without a remainder, for example, the GCD of 8 and 12 is 4. GCD is also known as ***Greatest Common Factor*** (GCF) or ***Highest Common Factor*** (HCF).
- **1- Computing GCD using Subtraction method:-**

- وهي أن تقوم بطرح العدد الأصغر من الأكبر لتحصل عل ناتج ثم تطرحه من العدد الأصغر في البداية وتكررعملية الطرح حتى تجد النتيجة صفر أي عندما يساوي a = b وعندها ذلك هو القاسم المشترك وكما ف المثالالتالي :-
- لحساب القاسم المشترك الاكبر (198,252)

Abs (252 – 198) = 54
Abs (198 – 54) = 144
Abs (144 - 54) = 90
Abs (90 – 54) = 36
Abs (54 - 36) =18
Abs (36 – 18) = 18
Abs (18 – 18) =0
∴ GCD (252,198) =18

Greatest Common Divisor(GCD).

2- Computing GCD using *Euclid's Algorithm* method:-

- Let *a* and *b* be two non-zero integers. The greatest common divisor of *a* and *b*, denoted gcd(a,b) is the largest of all common divisors of *a* and *b*.
- When gcd(*a*,*b*) = 1, we say that *a* and *b* are *relatively prime.*
- It can be calculated using the following equation: -***GCD*(a,b)=*GCD*(b,a mod b)**

- Euclid's Algorithm for computing GCD (a , b)
- A=a , B=b
- While B> 0
- R = A mod B
- A = B
- B = R
- Return A
- Example :- find the GCD(72,48).

GCD(89,25)=GCD(25, 89 mod 25)= GCD(25, 14)
GCD(25, 14)=GCD(14, 25 mod 14)= GCD(14,11)
GCD(14,11)=GCD(11, 14 mod 11)= GCD(11,3)
GCD(11,3)=GCD(3, 11 mod 3)=GCD(3, 2)
GCD(3,2)=GCD(2, 3 mod 2)=GCD(2,1)
GCD(2,1)=GCD(1, 2 mod 1)=GCD(1,0) so the GCD(89,25)=1

- ***Example* (1):-** Find GCD (123,4567) =1, GCD (27,18)=9

Least Common Multiple (LCM).

- The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b.
- The least common multiple of a and b is denoted by LCM(a, b).
- It can be calculated using the following equation: -

$$LCM(a, b) = |a * b| / GCD(a, b)$$

- Example :- find the LCM(354,144).

GCD(354,144)=GCD(144,354 mod 144)=GCD(144,66)

GCD(144,66)=GCD(66, 144 mod 66)= GCD(66,12)

GCD(66,12) =GCD(12, 66 mod 12)=GCD(12,6)

GCD(12,6)=GCD(6, 127 mod 6)=GCD(6,0)=6

LCM(354,143)=(354*144)/6=8496

Modular Arithmetic

- several important cryptosystems make use of modular arithmetic. This is when the answer to a calculation is always in the range 0 – *m* where m is the **modulus**.
- (a mod n) means the remainder when a is divided by n.
- a mod n = r
- a div n=q
- a = qn + r
- r = a – q * n

Example :- if a=13 and n=5, find q and r.

q=13 div 5=2 and r=13-2 *5=**3** which is equivalent to (13 mod 5)

Example :- find (-13 mod 5).

This can be found by find the number (b) where 5*b >13 then let b=3 and 5*3=15 which is less than 13 so

-13 mod 5=5*3-13=**2**

- Example: - Find the multiplicative inverse of 11 in Z_{26}.
- The GCD(26,11)must be 1 in order to find the inverse. Bu using the extended Euclidean algorithm, we can use this table

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

- the inverse of 11 is −7 mod 26=19.
- Or we can find the inverse based on using the equation $n = qn + r$

- Example: - Find the multiplicative inverse of 11 in Z_{26}.
- 26=11*2+4
- 11=4*2+3
- 4=3*1+1
- 3=3*1+0
- We are now in reverse compensation starting from one as shown
- 1=4-(3*1)
- 1=4-(11-(4*2))
- 1=4-11+4*2
- 1=3*4-11
- 1=3*(26-11*2)-11
- 1=3*26-6*11-11= 3*26-7*11 so the multiplicative inverse of 11 is -7

- Example :- Find the multiplicative inverse of 23 in Z_{100}.
- 100=23*4+8
- 23=8*2+7
- 8=7*1+1
- 7=1*7+0
- Now in revers way
- 1=8-(7*1)
- 1=8-(23-8*2)
- 1=8-23+8*2
- 1=3*8-23
- 1=3*(100-23*4)-23=3*100-12*23-23=3*100-13*23 So the multiplicative inverse of 23 in Z_{100} is -23 or 87(-23 mod 100).