زانكۆی سەلاحەددین - هەولێر
Salahaddin University-Erbil

# Information Security

## Lecture Four

## Introduction to Number Theory1


**Instructor: Newroz N. Abdulrazaq**

**Science College- Department of Computer Science & I.T.**

**newroz.abudlrazaq@su.edu.krd**


Text Book: William Stalling, Cryptography And Network Security Principles And Practice.+ Educational Websites.

# Overview:

- Division Theorem.
- Identity.
- Inverse.
- Factor (Divisor).
- Greatest Common Divisors (GCD).
- Modular Arithmetic.
- Solving Diophantine Equation.
- Finding inverse of a (mod n).

# Division Theorem

Let a and b be two integers with b>0, then there exists unique integers q and r satisfying: $a = qb + r$, where $r \geq 0$

Example: 17 and 5 are two Integers

$\therefore 17=3\times5+2$

a= 17 is Divisor.

b= 5 is Dividend.

q= 3 is Quotient.

r= 2 is Remainder.

$$\begin{array}{r|l} & 3 \\ \hline 5 & 17 \\ - & 15 \\ \hline & 2 \end{array}$$

# Division Theorem

Example: -20 and 7 are two Integers

$\therefore -20 = -3 \times 7 + 1$

$$\begin{array}{r|l} & \quad -3 \\ \hline 7 & \quad -20 \\ + & \quad \cancel{-}21 \\ \hline & \quad \cancel{0}1 \end{array}$$

a= -20 is Divisor.

b= 7 is Dividend.

q= -3 is Quotient.

r= 1 is Remainder.

# Identity

Let $\theta$ be any operation on numbers, a number i is called an identity for $\theta$ if $x \,\theta\, i = x$ and $i \,\theta\, x = x$ for every number x.

Example:

For Sum the identity is zero: $0+17=17$

For Multiplication the identity is one: $1 \times 25 = 25$

# Inverse

Let i be any identity for $\theta$, the number b is called the inverse of number a under $\theta$ if: $a\ \theta\ b = i$.

Example:

For Multiplication, the inverse of 25 is $\frac{1}{25}$:

$$\frac{1}{25} \times 25 = 1$$

# Factor (Divisor)

Let a and b are two integers and “b goes into a”, i.e. a=cb, where c is an integer, denoted by $b \mid a$ and say that b divides a or (that b is a factor of a).

Remark: We write $b \nmid a$ when b does not divide a.

Example: 5 is a factor of 20

$\therefore 20 = 4 \times 5$

$$\begin{array}{r|l} & 4 \\ \hline 5 & 20 \\ - & 20 \\ \hline & 0 \end{array}$$

$\therefore$ 5 is a factor of 20

# Greatest Common Divisors (GCD)

Given two integer numbers a and b, their greatest common divisor denoted by GCD(a,b) or (a, b), is the largest natural number which divides both of them, or in the other word we say GCD(a, b) = d iff:

1- $d | a$ and $d | b$.

2- if $c | a$ and $c | b$ then $c | d$ where c and d two integer numbers.

# GCD using Euclidean Algorithm

**Example**: Use Euclidean algorithm to find the GCD between 819 and 462.

$819 = 1 \times 462 + 357$

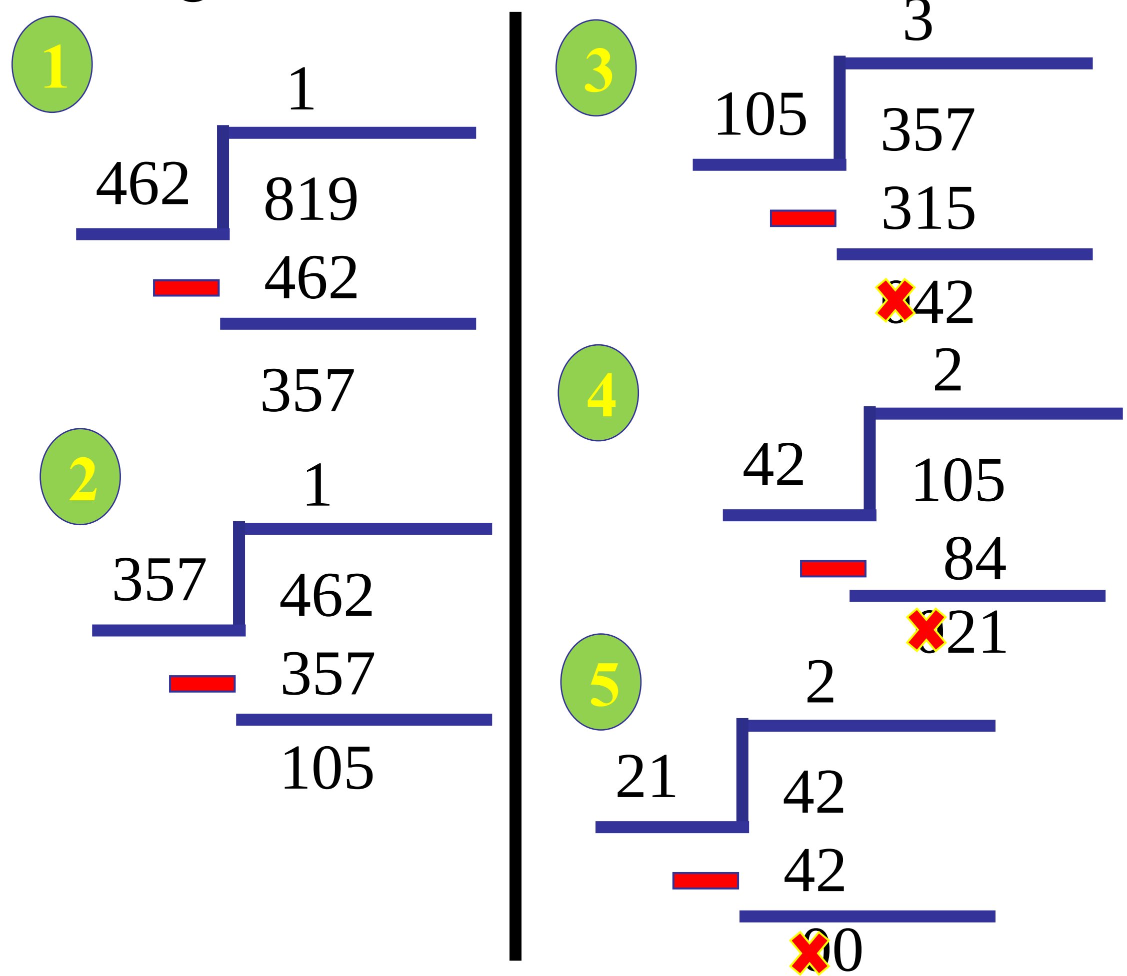
$462 = 1 \times 357 + 105$

$357 = 3 \times 105 + 42$

$105 = 2 \times 42 + 21$

$42 = 2 \times 21 + 0$

$\therefore GCD(819,462) = 21$



# Modular Arithmetic

Introduce as a way of confining results to a particular range.

Example:

$z_5=\{0, 1, 2, 3, 4\}$

$z_6=\{0, 1, 2, 3, 4, 5\}$

**Remarks**:

1. Modular arithmetic result stay in the underlying range number.

$8 \text{ in } z_5= ?$

$8 \bmod 5= 3$

# Modular Arithmetic… Cont.

$$\begin{array}{r|l} & 1 \\ \hline 5 & 8 \\ - & 5 \\ \hline & 3 \end{array} \quad \Rightarrow \quad 8 \bmod 5 = 3$$

**Remarks:**

2. The operations (+, -, *) can be applied before or after the modulus taken, with similar results.

Example: 17 +25=? in $z_6$

17 +25=42 mod 6=0 **or** 17 mod 6+25 mod 6=5+1=6 mod 6=0

# Modular Arithmetic… Cont.

**Remarks:**

3. Two integers are equivalents under modulus n if their results mod n are equal. i.e. $a \equiv_n b$ iff (a mod n) = (b mod n)

Example:

17 mod 8= 1 also 41 mod 8=1

so $17 \equiv_8 41$

# Modular Arithmetic… Cont.

**Remarks:**

4. Table below shows one way of computing the sum and product of any two integers mod 4 where:

$$a \bmod 4 = a - 4 * \text{int}\,(a / 4)$$

Sum

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Product

| $\times_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

# Solving Diophantine Equation

A very basic fact, is that, given integers a and b, there are integers x and y such that: $ax + by = GCD(a, b)$.

First Method: Extended Euclidean Method (Iteration Method):

Suppose we start by dividing a into b, so $b = q_i a + r_i$, and then proceed as in the Euclidean algorithm. Let the successive quotients be $q_1, q_2, \ldots, q_n$, so, we have the following sequences:

$$x_0 = 0,\ x_1 = 1,\ x_j = -\,q_{j-1}\, x_{j-1} + x_{j-2},$$

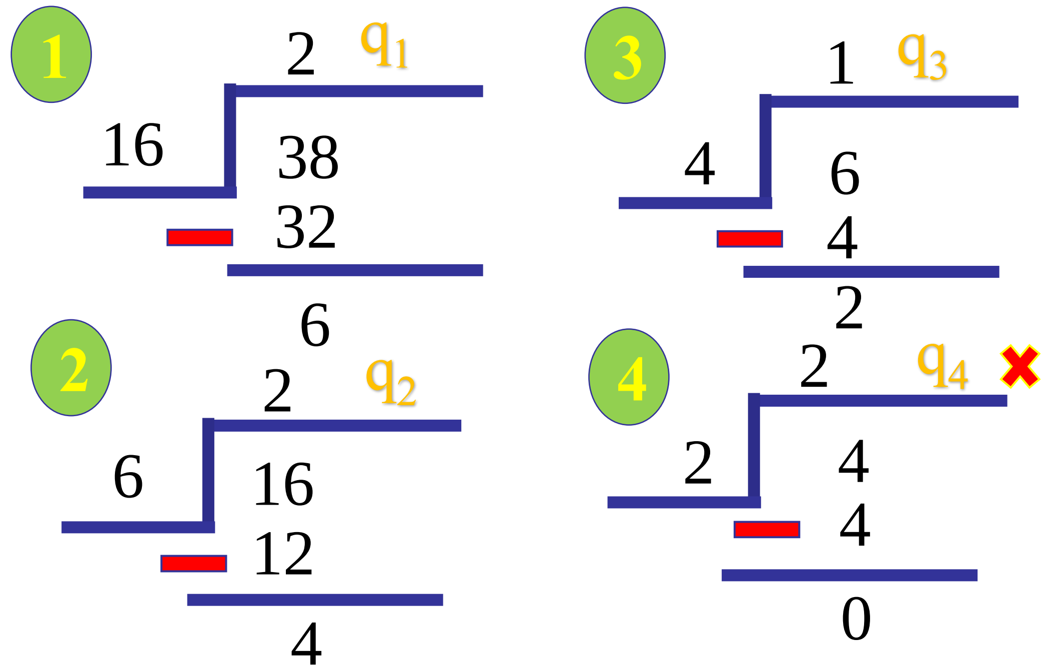
$$y_0 = 1,\ y_1 = 0,\ y_j = -\,q_{j-1}\, y_{j-1} + y_{j-2}. \quad \text{where } j=2, 3, \ldots$$

Remark: We did not use final quotient.

**Example**: Solve 16x+38y = gcd(16, 38)?

$$38 = 2 \times 16 + 6$$
$$16 = 2 \times 6 + 4$$
$$6 = 1 \times 4 + 2$$
$$4 = 2 \times 2 + 0$$

$$\therefore GCD(38, 16) = 2$$




$x_0 = 0,\ x_1 = 1,\ x_j = -\,q_{j-1}\, x_{j-1} + x_{j-2}$ where j=2, 3, 4

$x_2 = -\,q_1\, x_1 + x_0$ ⟺ $x_2 = -\,2 \times 1 + 0 = -2$

# Solution…Cont.

$x_3 = -q_2\, x_2 + x_1 \iff x_3 = -2 \times -2 + 1 = 5$

$x_4 = -q_3\, x_3 + x_2 \iff x_4 = -1 \times 5 + (-2) = -7$

$y_0 = 1,\ y_1 = 0,\ y_j = -q_{j-1}\, y_{j-1} + y_{j-2}$ where $j=2, 3, 4$

$y_2 = -q_1\, y_1 + y_0 \iff y_2 = -2 \times 0 + 1 = 1$

$y_3 = -q_2\, y_2 + y_1 \iff y_3 = -2 \times 1 + 0 = -2$

$y_4 = -q_3\, y_3 + y_2 \iff y_4 = -1 \times -2 + 1 = 3$

Checking: $16x+38y = \gcd(16, 38)=2$

$16 \times -7 + 38 \times 3 = -112+114=2$

**Example**: Solve 16x+38y = gcd(16, 38)?

$38 = 2 \times 16 + 6 \quad \Longleftrightarrow \quad 6 = 38 - 2(16)$

$16 = 2 \times 6 + 4 \quad \Longleftrightarrow \quad 4 = 16 - 2(6)$

$6 = 1 \times 4 + 2 \quad \Longleftrightarrow \quad 2 = 6 - 1(4)$

$4 = 2 \times 2 + 0$ ✗

$\therefore GCD(38, 16) = 2$

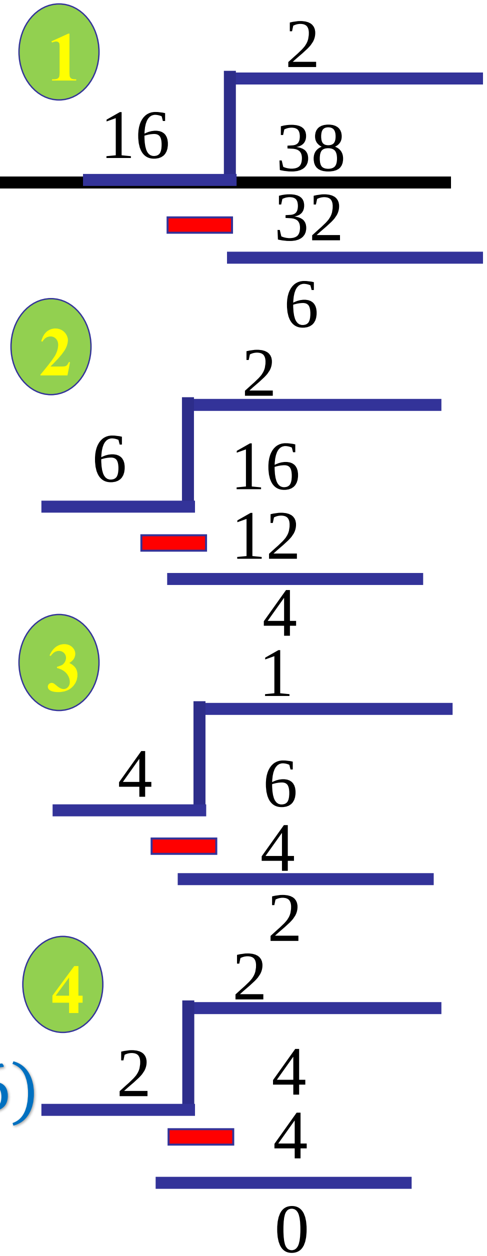
$2 = 6 - 1(4) = 6 - 1[16 - 2(6)]$

$= 6 - 1(16) + 2(6) = 3(6) - 1(16)$

$= 3[38 - 2(16)] - 1(16)$

$= 3(38) - 6(16) - 1(16) = 3(38) - 7(16)$

$\therefore$ x= -7 and y=3



# Finding inverse of a (mod n) [ $a^{-1}\ mod\ n$]

1) Use the extended Euclidean algorithm to find integers s and t such that as + n t = 1.
2) $a^{-1} \equiv s \pmod{n}$.

**Remarks**:

1. If the greater common divisor between two numbers equal to one i.e. GCD (a, b) = 1 then the inverse must be existing and unique, if GCD (a, b) $\neq$ 1 then the inverse is not unique.
2. To find the inverse using Euclidean algorithm we follow the same method for solving ax+by=gcd(a, b).

**Example**: Find the inverse of 5 mod 8.

$8 = 1 \times 5 + 3 \iff 3 = 8 - 1(5)$

$5 = 1 \times 3 + 2 \iff 2 = 5 - 1(3)$

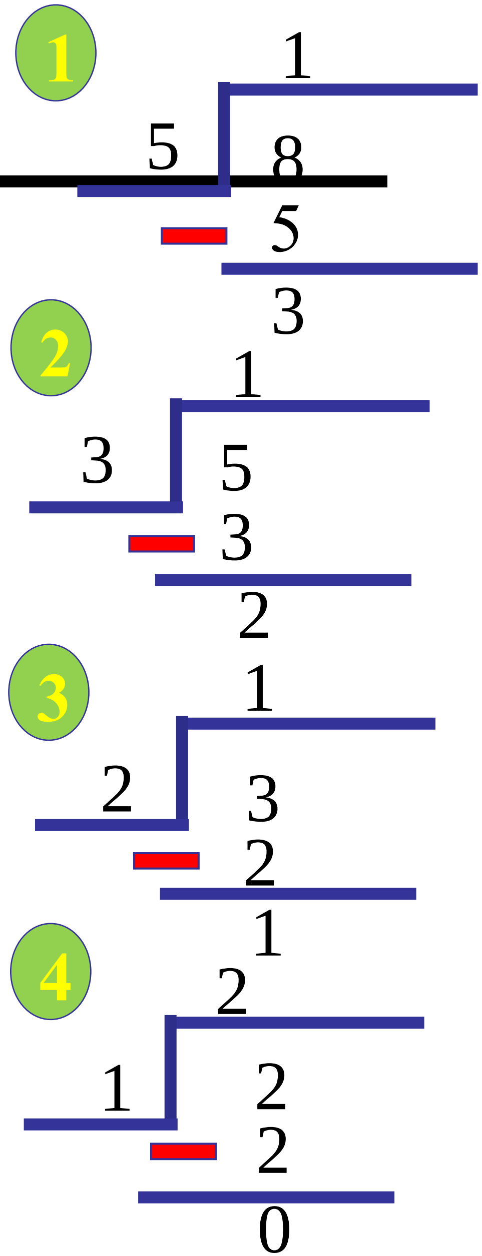
$3 = 1 \times 2 + 1 \iff 1 = 3 - 1(2)$

$2 = 2 \times 1 + 0$ ✗

$\therefore GCD(38, 16) = 1$

$$\begin{aligned} 1 &= 3 - 1(2) = 3 - 1[5 - 1(3)] \\ &= 3 - 1(5) + 1(3) = 2(3) - 1(5) \\ &= 2[8 - 1(5)] - 1(5) = 2(8) - 2(5) - 1(5) \\ &= 2(8) - 3(5) \end{aligned}$$

$\therefore$ **$5^{-1}$ mod 8= -3  mod 8= 5**



# Homework4

**Q1:** Find GCD between 512 and 1024 using three techniques?

**Q2:** Find the quotient and remainder for -311 and 17?

**Q3: C**ompute the sum and product of all integers mod 7?

**Q4:** Find inverse of 5 mod 8 using iteration method?

**Q5:** Find the inverse of 50 mod 71?