# MATHEMATICS OF CRYPTOGRAPHY
# PART I
# MODULAR ARITHMETIC AND CONGRUENCE

# Objectives

- To review integer arithmetic, concentrating on divisibility and finding the GCD using Euclidean algorithm.
- To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations.
- To solve linear congruent equations.
- To find additive and multiplicative inverses.
- To emphasize the importance of modular arithmetic and the modulo operators, because they are extensively used in cryptography.

# Book : Cryptography and Network security by Behrouz A. Forouzan

# Integer Arithmetic

- In integer arithmetic, we use a set and a few operations.
- Reviewed here to create a background for modular arithmetic.

# Set of Integers

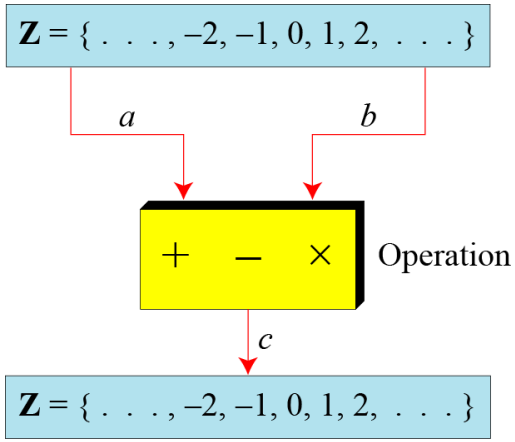
- The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity

$$\mathbf{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \}$$

***The set of integers***

# Binary Operations

- In cryptography, we are interested in three binary operations applied to the set of integers. division?
- A binary operation takes two inputs and creates one output.




***Three binary operations for the set of integers***

# Integer Division

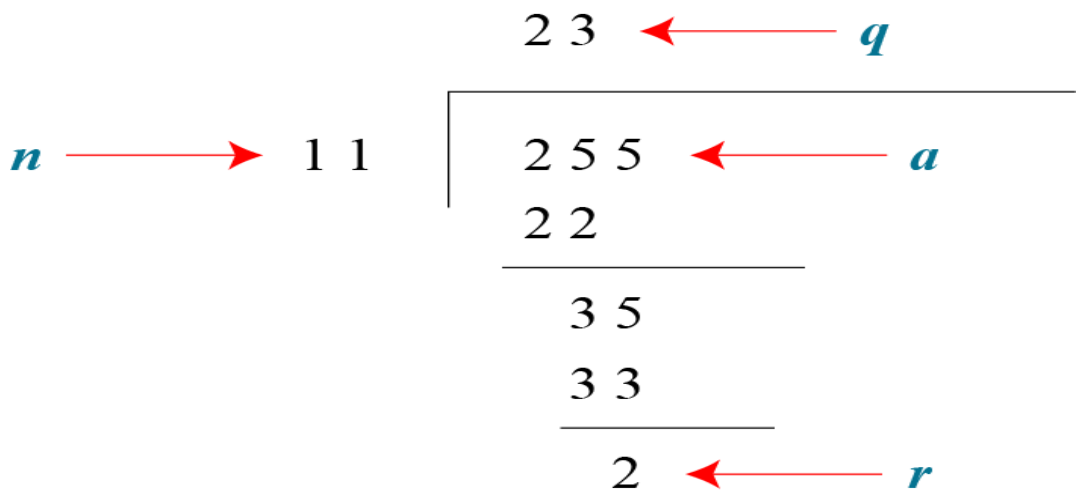
- In integer arithmetic, if we divide a by n, we can get q and r.
- The relationship between these four integers can be shown as

$$a = q \times n + r$$

**a=** dividend
n= divisor
**q=** quotient
r= remainder

# Integer Division(cont.)

- Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm.



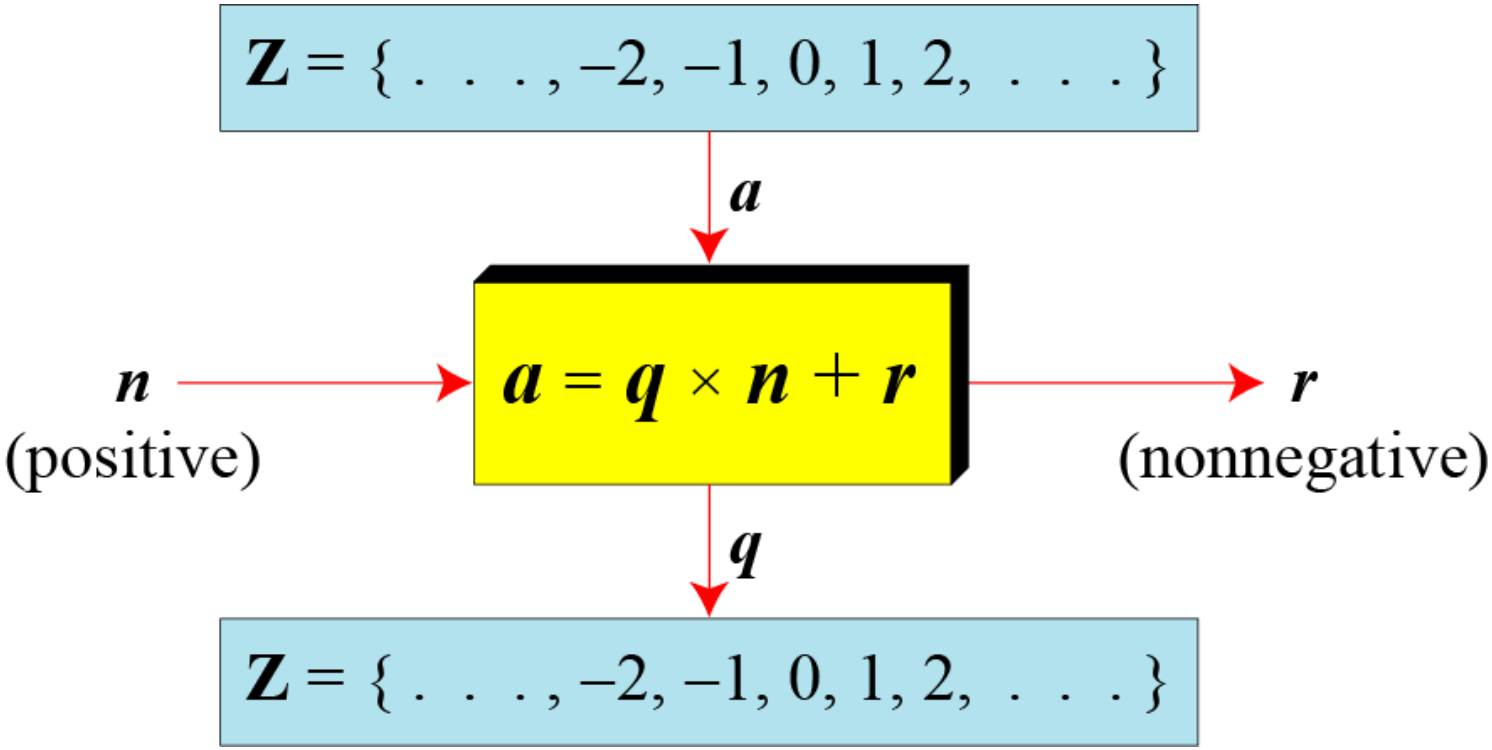

***Finding the quotient and the remainder***

- How to find the *quotient* and the *remainder* using language specific operators??? <in case of C language>

# Integer Division(cont.)

In case of division relationship in cryptography, we impose two restrictions.

1. We require that divisor be a positive integer ( $n > 0$ )
2. We require that the remainder be a nonnegative integer ( $r \geq 0$)




***Division algorithm for integers***

# Integer Division(cont.)

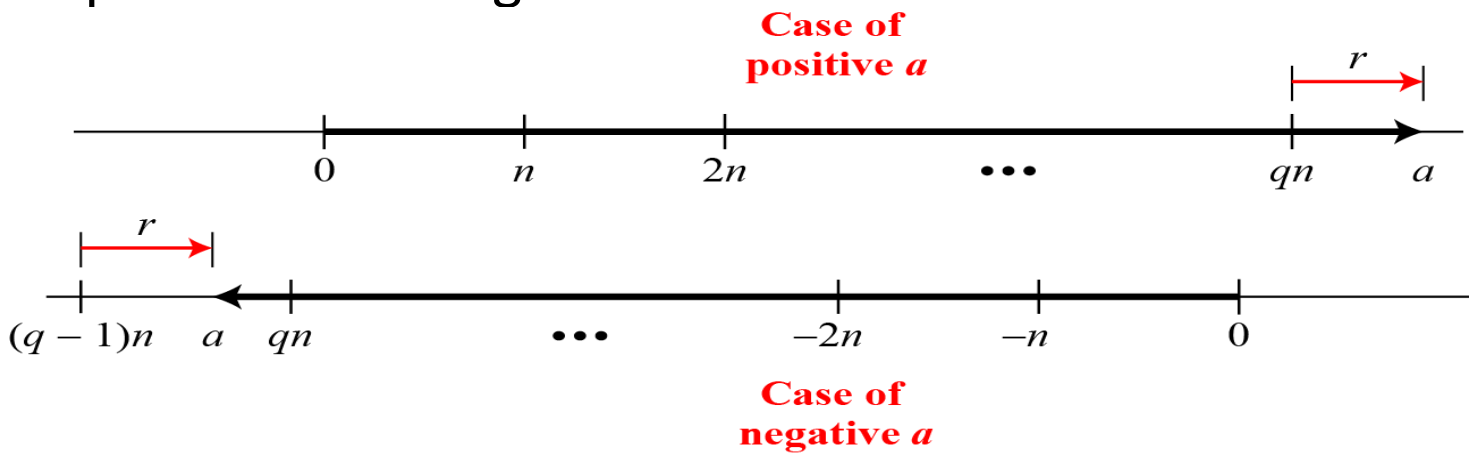
- When we use a computer or a calculator, r and q are negative when a is negative.
- How can we apply the restriction that r needs to be positive?
- The solution is simple, we decrement the value of q by 1 and we add the value of n to r to make it positive.

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

- The above relation is still valid.

# Integer Division(cont.)

- Graph of division algorithm




- If a is positive- move q×n units to right and move extra r units in the same direction.
- If a is negative- move (q-1)×n units to the left (q is negative in this case) and then r units in the opposite direction. <in both cases the value of r is positive>

# Divisibility

- If a is not zero and we let r = 0 in the division relation, we get

$$a = q \times n$$

- If the remainder is zero, $n \mid a$ (*n* divides a)

- If the remainder is not zero, $n \nmid a$ *(n does not divides a)*

# Divisibility(cont.)

- Properties

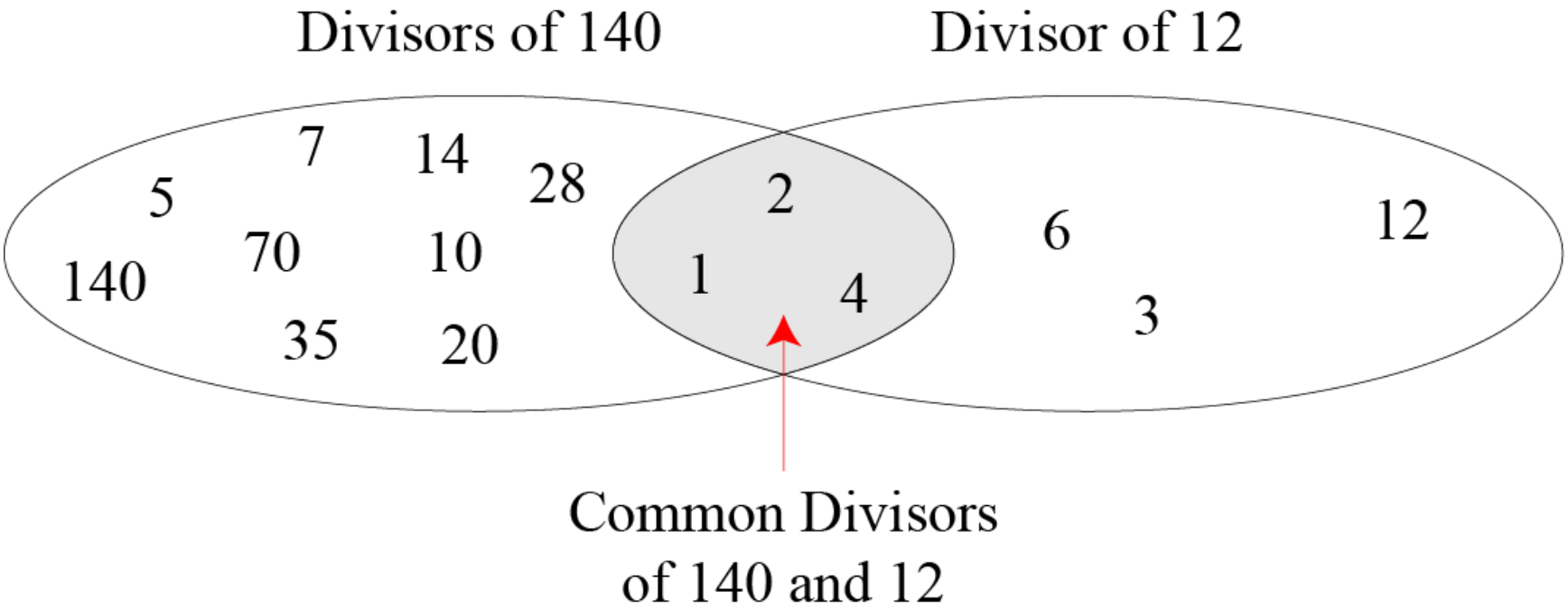
**Property 1: if a|1, then a = ±1.**

**Property 2: if a|b and b|a, then a = ±b.**

**Property 3: if a|b and b|c, then a|c.**

**Property 4: if a|b and a|c, then a|(m × b + n × c), where m and n are arbitrary integers**

# Divisibility(cont.)




***Common divisors of two integers***

# Divisibility(cont.)

**Greatest Common Divisor**

*The greatest common divisor of two positive integers is the largest integer that can divide both integers.*

**Euclidean Algorithm**

*Fact 1: gcd (a, 0) = a*
*Fact 2: gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b*

# Divisibility(cont.)

- For example, to calculate the gcd(36,10), we use following steps:

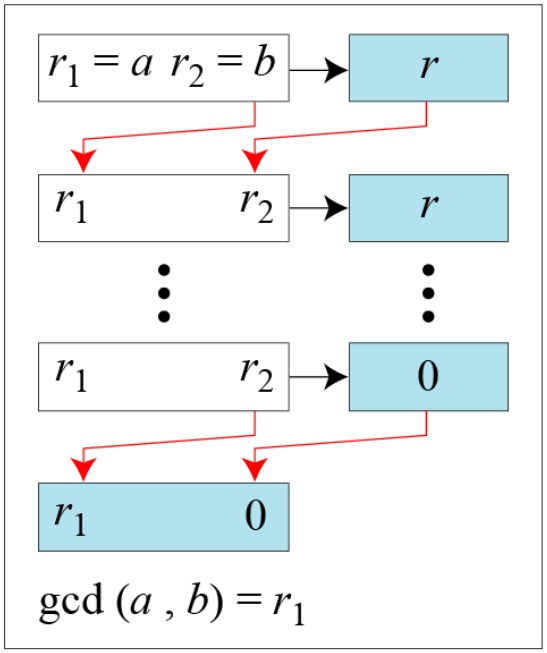
*gcd (36, 10) = gcd (10, 6).....by fact 2*
*gcd (10, 6) = gcd (6, 4).....by fact 2*
*gcd (6, 4) = gcd (4, 2).....by fact 2*
*gcd (4, 2) = gcd (2, 0).....by fact 2*
*gcd (2, 0) = 2.....by fact 1*

*Hence, Answer = 2*

# Divisibility(cont.)

***Euclidean Algorithm:***

***- Two variables, r1 and r2, to hold the changing values during the process of reduction.***




a. Process

$r_1 \leftarrow a; \quad r_2 \leftarrow b;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

**When gcd (a, b) = 1, we say that a and b are relatively prime.**

# Divisibility(cont.)

Find the greatest common divisor of 2740 and 1760.

| $q$ | $r_1$ | $r_2$ | $r$ |
|---|---|---|---|
| 1 | 2740 | 1760 | 980 |
| 1 | 1760 | 980 | 780 |
| 1 | 980 | 780 | 200 |
| 3 | 780 | 200 | 180 |
| 1 | 200 | 180 | 20 |
| 9 | 180 | 20 | 0 |
| | **20** | 0 | |

Answer: gcd (2740, 1760) = 20.

# Divisibility(cont.)

Find the greatest common divisor of 25 and 60.

# Divisibility(cont.)

## Extended Euclidean Algorithm

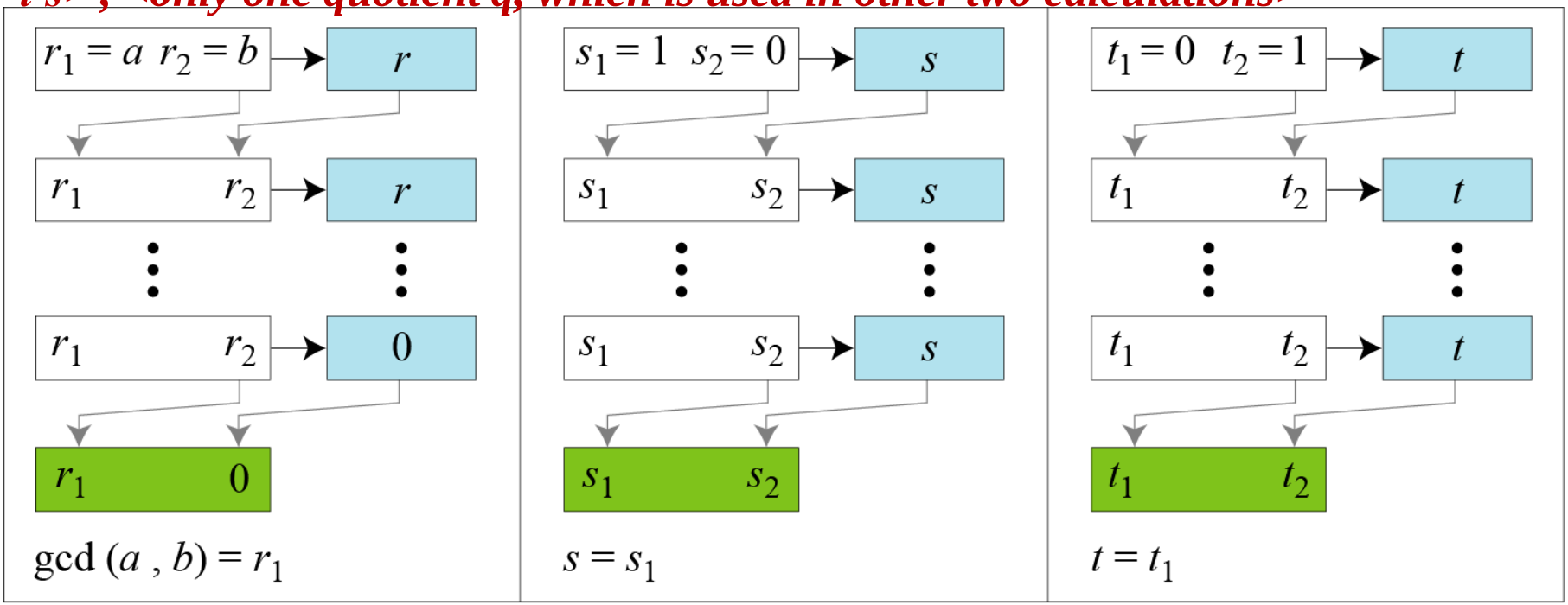
Given two integers *a* and *b*, we often need to find other two integers, *s* and *t*, such that

$$s \times a + t \times b = \gcd(a, b)$$

The extended Euclidean algorithm can calculate the gcd (*a*, *b*) and at the same time calculate the value of *s* and *t*.

# Divisibility(cont.)

***Extended Euclidean algorithm, part a-*** ***<use of three set of variables, r's, s's, and t's>*** **,** ***<only one quotient q, which is used in other two calculations>***




a. Process

# Divisibility(cont.)

***Extended Euclidean algorithm, part b***

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating $r$'s)

$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating $s$'s)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating $t$'s)

}

gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

b. Algorithm

# Divisibility(cont.)

Given $a = 161$ and $b = 28$, find gcd $(a, b)$ and the values of $s$ and $t$.

**Solution**

| $q$ | $r_1$ | $r_2$ | $r$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|---|---|---|
| 5 | 161 | 28 | 21 | 1 | 0 | 1 | 0 | 1 | −5 |
| 1 | 28 | 21 | 7 | 0 | 1 | −1 | 1 | −5 | 6 |
| 3 | 21 | 7 | 0 | 1 | −1 | 4 | −5 | 6 | −23 |
| | **7** | 0 | | **−1** | 4 | | **6** | −23 | |

We get gcd (161, 28) = 7, $s = -1$ and $t = 6$.

# Divisibility(cont.)

Given $a$ = 17 and $b$ = 0, find gcd ($a$, $b$) and the values of $s$ and $t$.

**Solution**

| $q$ | $r_1$ | $r_2$ | $r$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|---|---|---|
| | **17** | 0 | | **1** | **0** | | **0** | **1** | |

We get gcd (17, 0) = 17, $s$ = 1, and $t$ = 0

# Divisibility(cont.)

Given $a$ = 0 and $b$ = 45, find gcd ($a$, $b$) and the values of $s$ and $t$.

**Solution**

| $q$ | $r_1$ | $r_2$ | $r$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 45 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | **45** | 0 | | 0 | 1 | | **1** | 0 | |

We get gcd (0, 45) = 45, $s$ = 0, and $t$ = 1.

# Divisibility(cont.)

**Exercise:**

Given $a$ = 84 and $b$ = 320, find gcd ($a$, $b$) and the values of $s$ and $t$.

# Divisibility(cont.)

**Exercise:**

Given $a$ = 84 and $b$ = 320, find gcd ($a$, $b$) and the values of $s$ and $t$.

**Solution:**

gcd(84,320) = 4, s = -19, t = 5

# Linear Diophantine Equations

- **A linear Diophantine equation of two variables is,**
  **ax + by = c.**

- **We want to find integer values for x and y that satisfy the equation.**
- **Either no solution or an infinite number of solutions**
- **Let d = gcd(a,b); if d $\nmid$ c, the equation has no solution.**
- **If d | c, the equation has infinite number of solutions : one of them is particular and the rest are general**

# Linear Diophantine Equations(cont.)

**Particular Solution:** **ax + by = c**

**If d | c, a particular solution to the above equation can be found using Following steps:**

1. **Reduce the equation to $a_1x + b_1y = c_1$ by dividing both sides of the equation by d. This is possible because d divides a, b, and c by the assumption.**
2. **Solve for s and t in the relation $a_1s + b_1t = 1$ using the extended Euclidean Algorithm.**
3. **The particular solution can be found:**

***Particular solution:***
***$x_0$ = (c/d)s and $y_0$ = (c/d)t***

# Linear Diophantine Equations(cont.)

**General Solution:**

**After finding the particular solution, the general solutions can be found:**

***General solutions:***
***$x = x_0 + k\,(b/d)$ and $y = y_0 - k(a/d)$***
***where k is an integer***

# Linear Diophantine Equations(cont.)

**Example:**

Find the particular and general solutions for the equation

21x + 14y = 35.

***Particular solution:***
***$x_0$ = (c/d)s and $y_0$ = (c/d)t***

***General solutions:***
***x = x0 + k (b/d) and y = y0 − k(a/d)***
***where k is an integer***

# Linear Diophantine Equations(cont.)

**Example:**

Find the particular and general solutions for the equation

21x + 14y = 35.

***Particular solution:***
***$x_0$ = (c/d)s and $y_0$ = (c/d)t***

***General solutions:***
***x = x0 + k (b/d) and y = y0 − k(a/d)***
***where k is an integer***

**Solution:**

d= gcd (21,14)= 7, since 7|35

We have s=1 and t= -1

Particular solution: ($x_0$, $y_0$) = (5, -5)

General solutions : (5,-5), (7,-8), (9,-11) …

# Linear Diophantine Equations(cont.)

**Example:**

Imagine we want to cash a Rs.100 cheque and get some Rs.20 notes and some Rs.5 notes.

Find out the possible choices if any exist for the given problem

***Particular solution:***
***$x_0 = (c/d)s$ and $y_0 = (c/d)t$***

***General solutions:***
***$x = x0 + k\,(b/d)$ and $y = y0 - k(a/d)$***
***where k is an integer***

# Linear Diophantine Equations(cont.)

***Particular solution:***
***$x_0 = (c/d)s$ and $y_0 = (c/d)t$***

***General solutions:***
***$x = x0 + k\,(b/d)$ and $y = y0 - k(a/d)$***
***where k is an integer***

**Solution:**

**20 x+ 5 y= 100**

**Since d= gcd(20,5) and 5 divides 100**

**Divide both sides by 5 to get 4x +y= 20**

**Then solve the equation**

**4s+ t= 1**

**Where,**

**S=0, and t=1 using the extended Euclidean algorithm**

**The particular solutions are** $x_0 = 0 \times 20 = 0$ and $y_0 = 1 \times 20 = 20$

The general solutions with x and y nonnegative are (0, 20), (1,16), (2, 12), (3, 8), (4, 4), (5, 0)

# Modular Arithmetic

# Preliminary

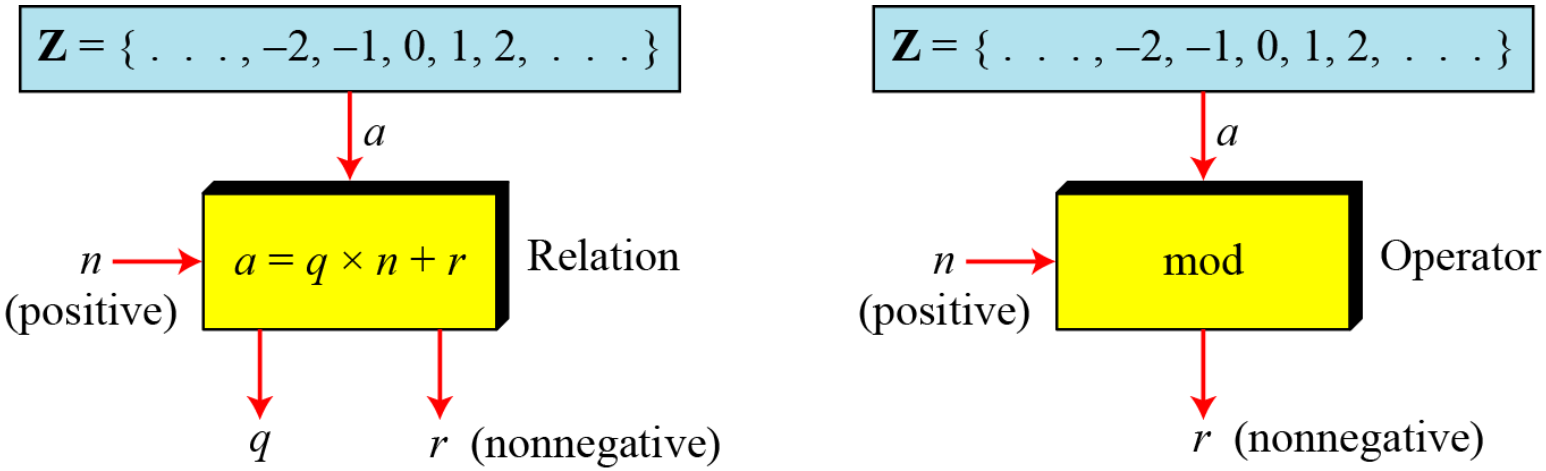
- The division relationship ($a = q \times n + r$) discussed in the previous section has two inputs (a and n) and two outputs (q and r).
- In modular arithmetic, we are interested in only one of the outputs, the remainder r.

# Preliminary(cont.)

- We use modular arithmetic in our daily life; for example, we use a clock to measure time. Our clock system uses modulo 12 arithmetic.

# Modulo Operator

- The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.




***Division algorithm and modulo operator***

# Modulo Operator(cont.)

- Find the result of the following operations:

a. 27 mod 5

b. 36 mod 12

c. −18 mod 14

d. −7 mod 10

# Modulo Operator(cont.)

- Solution

a. Dividing 27 by 5 results in r = 2

b. Dividing 36 by 12 results in r = 0

c. Dividing −18 by 14 results in r = −4. After adding the modulus r = 10

d. Dividing −7 by 10 results in r = −7. After adding the modulus to −7, r = 3

# Set of Residues : $Z_n$

- The results of the modulo operation with modulus *n* is always an integer between 0 and n-1. <i.e. result of a mod n is always a nonnegative integer >
- The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or $Z_n$.

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

$\mathbf{Z}_2 = \{ 0, 1 \}$ $\mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}$ $\mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$

***Some $Z_n$ sets***

# Congruence

- In *cryptography,* we often used the concept of **congruence** instead of equality.
- To show that two integers are congruent, we use the congruence operator ( ≡ ).
- We say that a is congruent to b modulo m, and we write a ≡ b mod m, if m divides b-a.
- Example:

$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

# Congruence(cont.)

- Congruence operator Vs. equality operator
  - A equality operator maps a member of $\mathbf{Z}$ to itself,
  - The congruence operator maps a member from $\mathbf{Z}$ to member of $\mathbf{Z_n}$.
  - The equality operator is one-to-one,
  - The congruence operator is many-to-one

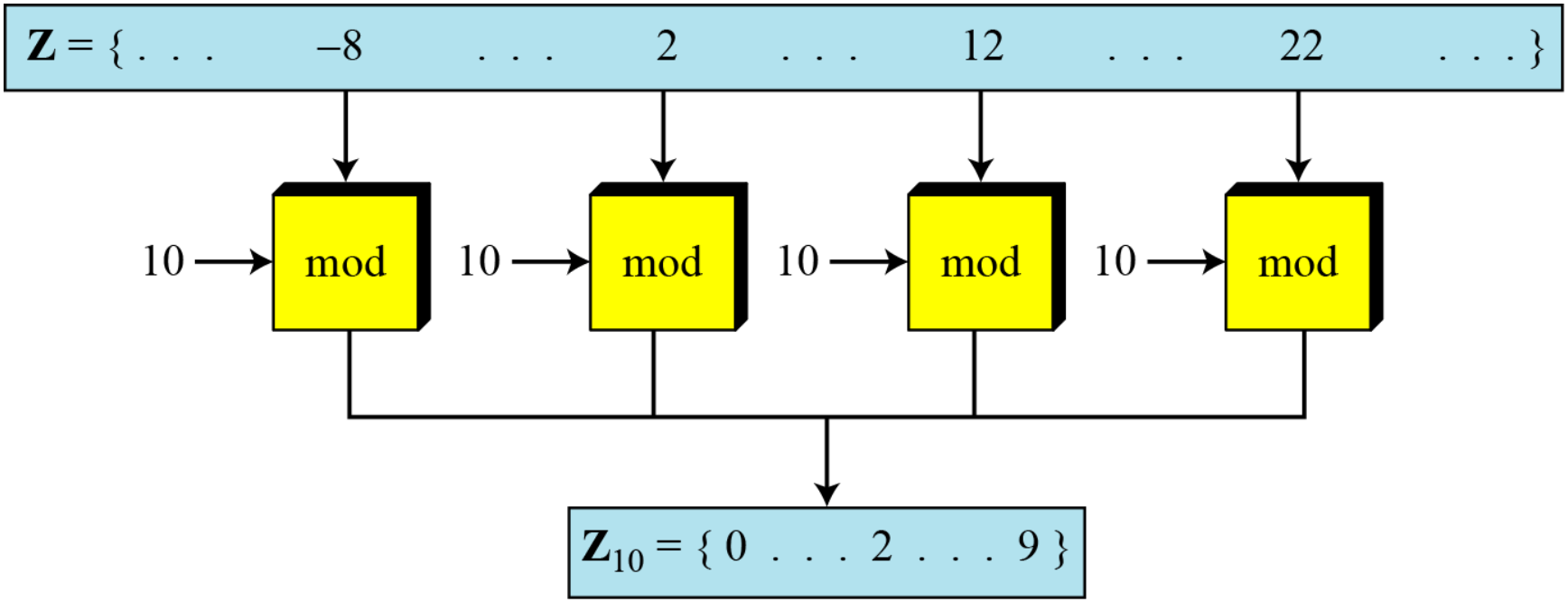
- The phrase *(mod* n*)* is an indication of destination set $\mathbf{Z_n}$. <Example- $\mathbf{2 \equiv 12 \pmod{10}}$, means that the destination set is $\mathbf{Z_{10}}$.>

# Congruence(cont.)

**Properties-**

- **$a \equiv b \bmod m$, implies that $b \equiv a \bmod m$** ***(symmetry)***
- **$a \equiv b \bmod m$ and $b \equiv c \bmod m$, implies that $a \equiv c \bmod m$** ***(transitivity)***

# Congruence(cont.)

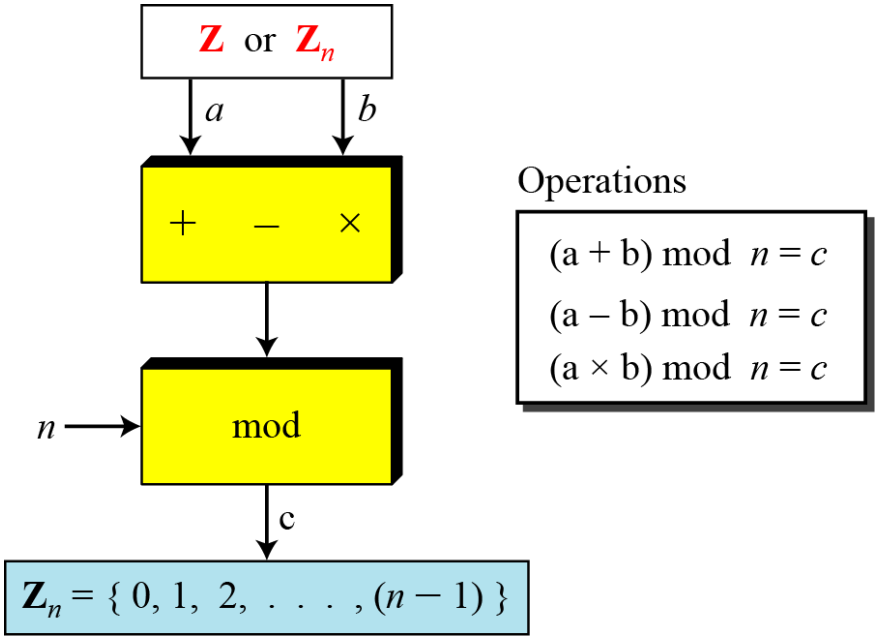



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

# Operation in Zn

- The three binary operations that we discussed for the set Z can also be defined for the set Zn. The result may need to be mapped to Zn using the mod operator.



# Operation in $Z_n$(cont.)

- Perform the following operations (the inputs come from $Z_n$):

a. Add 7 to 14 in $Z_{15}$.

b. Subtract 11 from 7 in $Z_{13}$.

c. Multiply 11 by 7 in $Z_{20}$.

# Operation in $Z_n$(cont.)

- Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

# Operation in $Z_n$(cont.)

- Perform the following operations (the inputs come from either Z or $Z_n$):

a. Add 17 to 27 in $Z_{14}$.

b. Subtract 43 from 12 in $Z_{13}$.

c. Multiply 123 by −10 in $Z_{19}$.

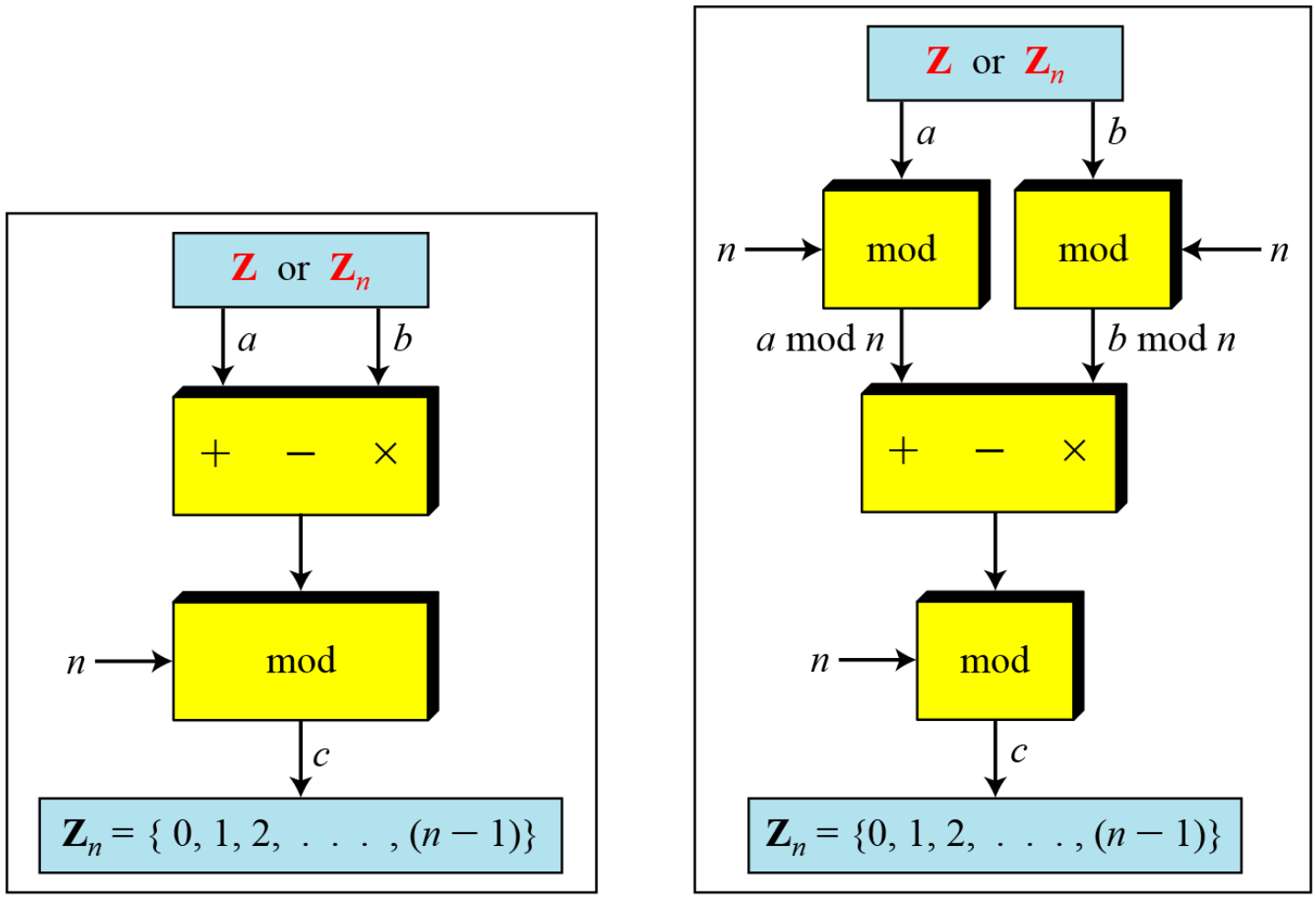
# Operation in $Z_n$(cont.)

- Solution
- Add 17 to 27 in $Z_{14}$.
  - (17+27)mod 14 = 2
- Subtract 43 from 12 in $Z_{13}$.
  - (12-43)mod 13 = 5
- Multiply 123 by −10 in $Z_{19}$.
  - (123 x (-10)) mod 19 = 5

# Operation in $Z_n$(cont.)

| | |
|---|---|
| **First Property:** | $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$ |
| **Second Property:** | $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$ |
| **Third Property:** | $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$ |

# Operation in $Z_n$(cont.)



# Operation in $Z_n$(cont.)

- The following shows the application of the above properties:

1. (1,723,345 + 2,124,945) mod 11 = (8 + 9) mod 11 = 6

2. (1,723,345 − 2,124,945) mod 16 = (8 − 9) mod 11 = 10

3. (1,723,345 × 2,124,945) mod 16 = (8 × 9) mod 11 = 6

# Inverses

- Working in modular arithmetic, we often need to find the inverse of a number relative to an operation.
- additive inverse (relative to an addition operation) or
- a multiplicative inverse (relative to a multiplication operation).

# Inverses- relevancy with cryptography

- In cryptography we often work with inverses.
- If the sender uses an integer (as the encryption key), the receiver uses the inverse of that integer (as the decryption key).
- If the operation (encryption/decryption algorithm) is addition, **Zn** can be used as the set of possible keys because each integer in this set has an additive inverse.
- On the other hand, if the operation (encryption/decryption algorithm) is multiplication , **Zn** cannot be the set of possible keys because only some numbers of this set have a multiplicative inverse.

# Additive Inverses

- In $Z_n$, two numbers a and b are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

**In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n.**

# Additive Inverses

- Find additive inverse of 4 in $Z_{10}$.
- Solution
  - In $Z_n$ , the additive inverse of a can be calculated as b=n – a.
  - The additive inverse 4 in $Z_{10}$ is 10-4=6 .

# Additive Inverses

- Find all additive inverse pairs in $Z_{10}$.
- Solution
  - The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

# Multiplicative Inverses

- In $Z_n$, two numbers a and b are the multiplicative inverse of each other if,

$$a \times b \equiv 1 \pmod{n}$$

**In modular arithmetic, an integer may or may not have a multiplicative inverse.**
**When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo n.**

# Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 8 in $Z_{10}$.
  - There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 1.
  - In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.
- Find all multiplicative inverses in $Z_{10}$.
  - There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

# Multiplicative Inverses(cont.)

- Find all multiplicative inverse pairs in $Z_{11}$.

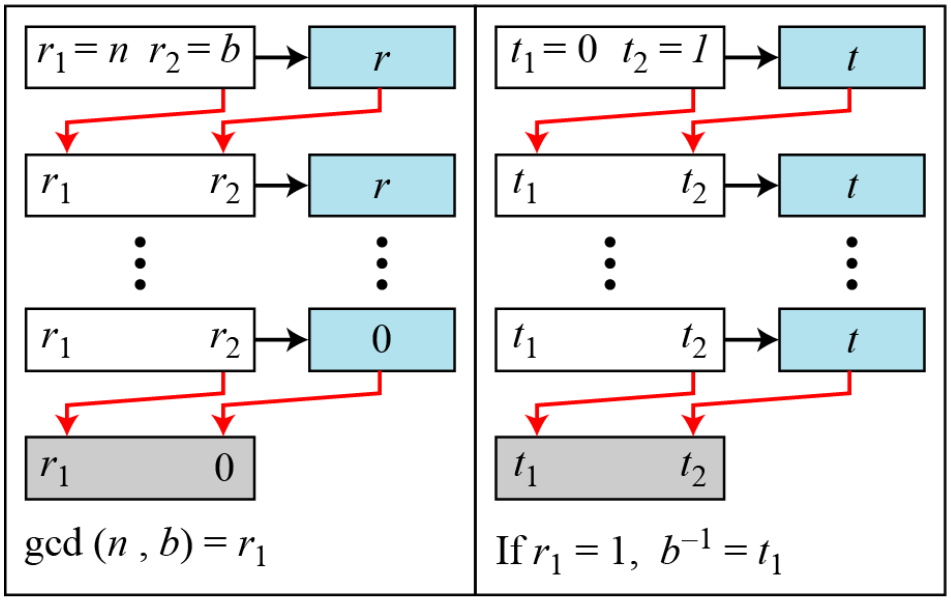
# Multiplicative Inverses(cont.)

- Find all multiplicative inverse pairs in $Z_{11}$.
  - Solution
    - We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 9), and (10, 10).
    - The reason is that in $Z_{11}$ , gcd (11,a) is 1 (relatively prime) for all value of a except 0. it means all integers 1 to 10 have multiplicative inverse.

# Multiplicative Inverses(cont.)

- The extended Euclidean algorithm finds the multiplicative inverses of b in $Z_n$ when *n* and *b* are given and *gcd (n, b) = 1*.
- The multiplicative inverse of *b* is the value of $t_1$ after being mapped to $Z_n$.

# Multiplicative Inverses




a. Process

$r_1 \leftarrow n;$ $r_2 \leftarrow b;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$

while $(r_2 > 0)$
{
$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow t;$

}
if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

b. Algorithm

***Using extended Euclidean algorithm to find multiplicative inverse***

# Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 11 in $Z_{26}$.

**Solution**

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| 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 gcd (26, 11) is 1; the inverse of 11 is -7 or 19.

# Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 23 in $Z_{100}$.

# Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 23 in $Z_{100}$.

Solution

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| 4 | 100 | 23 | 8 | 0 | 1 | –4 |
| 2 | 23 | 8 | 7 | 1 | –4 | 19 |
| 1 | 8 | 7 | 1 | –4 | 9 | –13 |
| 7 | 7 | 1 | 0 | 9 | –13 | 100 |
| | 1 | 0 | | –13 | 100 | |

The gcd (100, 23) is 1; the inverse of 23 is -13 or 87.

# Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 12 in $Z_{26}$.

**Solution**

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| 2 | 26 | 12 | 2 | 0 | 1 | –2 |
| 6 | 12 | 2 | 0 | 1 | –2 | 13 |
| | 2 | 0 | | –2 | 13 | |

The gcd (26, 12) is 2; the inverse does not exist.

# Addition and Multiplication Tables

- Addition and multiplication table for $Z_{10}$
- Additive Inverse: Inverse pair can be found when the result of addition is zero.
- Multiplicative Inverse: Inverse pair can be found when the result of multiplication is 1.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | **0** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | **0** |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | **0** | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | **0** | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 8 | 9 | **0** | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 8 | 9 | **0** | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 8 | 9 | **0** | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 8 | 9 | **0** | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 8 | 9 | **0** | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 9 | **0** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Addition Table in $\mathbf{Z}_{10}$

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2 | 0 | 2 | 4 | 6 | 8 | 0 | 2 | 4 | 6 | 8 |
| 3 | 0 | 3 | 6 | 9 | 2 | 5 | 8 | **1** | 4 | 7 |
| 4 | 0 | 4 | 8 | 2 | 6 | 0 | 4 | 8 | 2 | 6 |
| 5 | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 |
| 6 | 0 | 6 | 2 | 8 | 4 | 0 | 6 | 2 | 8 | 4 |
| 7 | 0 | 7 | 4 | **1** | 8 | 0 | 2 | 9 | 6 | 3 |
| 8 | 0 | 8 | 6 | 4 | 2 | 0 | 8 | 6 | 4 | 2 |
| 9 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | **1** |

Multiplication Table in $\mathbf{Z}_{10}$

# Different Sets of Addition and Multiplication

- Some $Z_n$ and $Z_n*$ sets

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbf{Z}_6^* = \{1, 5\}$

$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$

**We need to use $Z_n$ when additive inverses are needed; we need to use $Z_n*$ when multiplicative inverses are needed.**

# Linear Congruence

***Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in $Z_n$. This section shows how to solve equations when the power of each variable is 1 (linear equation).***

***Topics discussed in this section:***

**2.4.1 Single-Variable Linear Equations**

**2.4.2 Set of Linear Equations**

# Single-Variable Linear Equations

***Equations of the form ax ≡ b (mod n ) might have no solution or a limited number of solutions.***

Assume that the gcd $(a, n) = d$.

If $d \nmid b$, there is no solution.

If $d | b$, there are $d$ solutions.

# Continued

If d | b, we use the following strategy to find the solutions.

1. Reduce the equation by dividing both sides of the equation (including the modulus) by d.
2. Multiply both sides of the reduced equation by the multiplicative inverse of a to find the particular solution $x_0$.
3. The general solutions are $x_1 = x_0 + k\,(n/d)$ for k=0, 1,…..(d-1).

# Continued

**Example**

**Solve the equation 10 $x \equiv 2 \pmod{15}$.**

**Solution**

**First we find the gcd (10 and 15) = 5. Since 5 does not divide 2, we have no solution.**

**Example**

**Solve the equation 14 $x \equiv 12 \pmod{18}$.**

**Solution**

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \quad x \equiv 6\,(7^{-1}) \pmod{9}$$

$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$

$$x_1 = x_0 + 1 \times (18/2) = 15$$

# Continued

**Example**

**Solve the equation $3x + 4 \equiv 6 \pmod{13}$.**

**Solution**

**First we change the equation to the form $ax \equiv b \pmod{n}$. We add $-4$ (the additive inverse of 4) to both sides, which give $3x \equiv 2 \pmod{13}$. Because gcd (3, 13) = 1, the equation has only one solution, which is $x_0 = (2 \times 3^{-1}) \bmod 13 = 18 \bmod 13 = 5$. We can see that the answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.**

# Set of Linear Equations

***We can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible.***

**Figure 2.27** *Set of linear equations*

$$\begin{aligned}
a_{11}x_1 &+ a_{12}x_2 + \ldots + a_{1n}x_n \equiv b_1 \\
a_{21}x_1 &+ a_{22}x_2 + \ldots + a_{2n}x_n \equiv b_2 \\
&\vdots \qquad\quad \vdots \qquad\qquad \vdots \quad \vdots \\
a_{n1}x_1 &+ a_{n2}x_2 + \ldots + a_{nn}x_n \equiv b_n
\end{aligned}$$

a. Equations

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \qquad \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}^{-1} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

b. Interpretation c. Solution

# Continued

**Example**

**Solve the set of following three equations:**

$$3x + 5y + 7z \equiv 3 \pmod{16}$$
$$x + 4y + 13z \equiv 5 \pmod{16}$$
$$2x + 7y + 3z \equiv 4 \pmod{16}$$

**Solution**

**The result is $x \equiv 15 \pmod{16}$, $y \equiv 4 \pmod{16}$, and $z \equiv 14 \pmod{16}$. We can check the answer by inserting these values into the equations.**