Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

Lecture – 3: Introduction to Cryptography Mathematics

Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

Integer Arithmetic

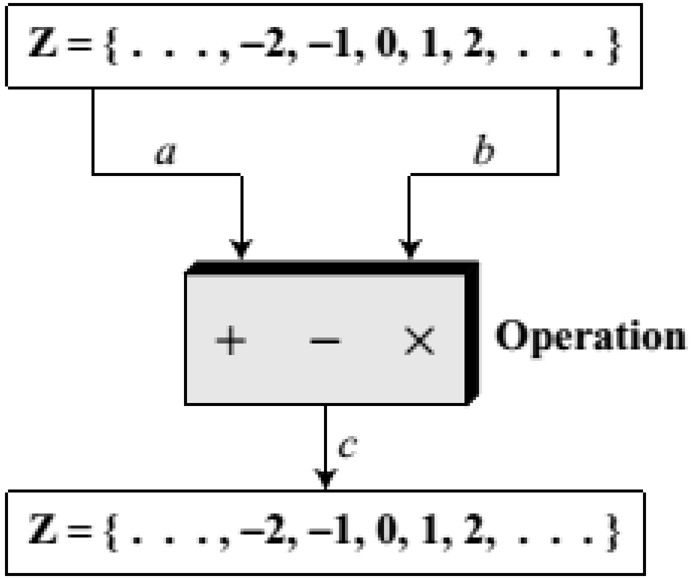
- In integer arithmetic, we use a set and a few operations.
- Reviewed here to create a background for modular arithmetic.
- The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity

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

The set of integers

Binary Operations

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



Example #1

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

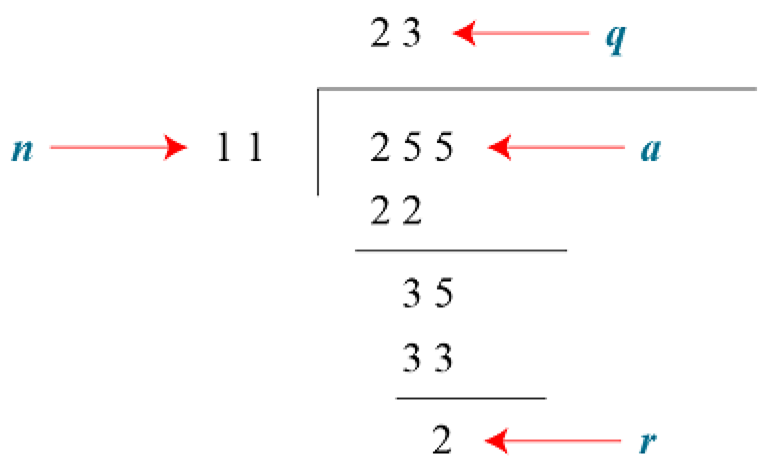
Integer Division

- 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

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

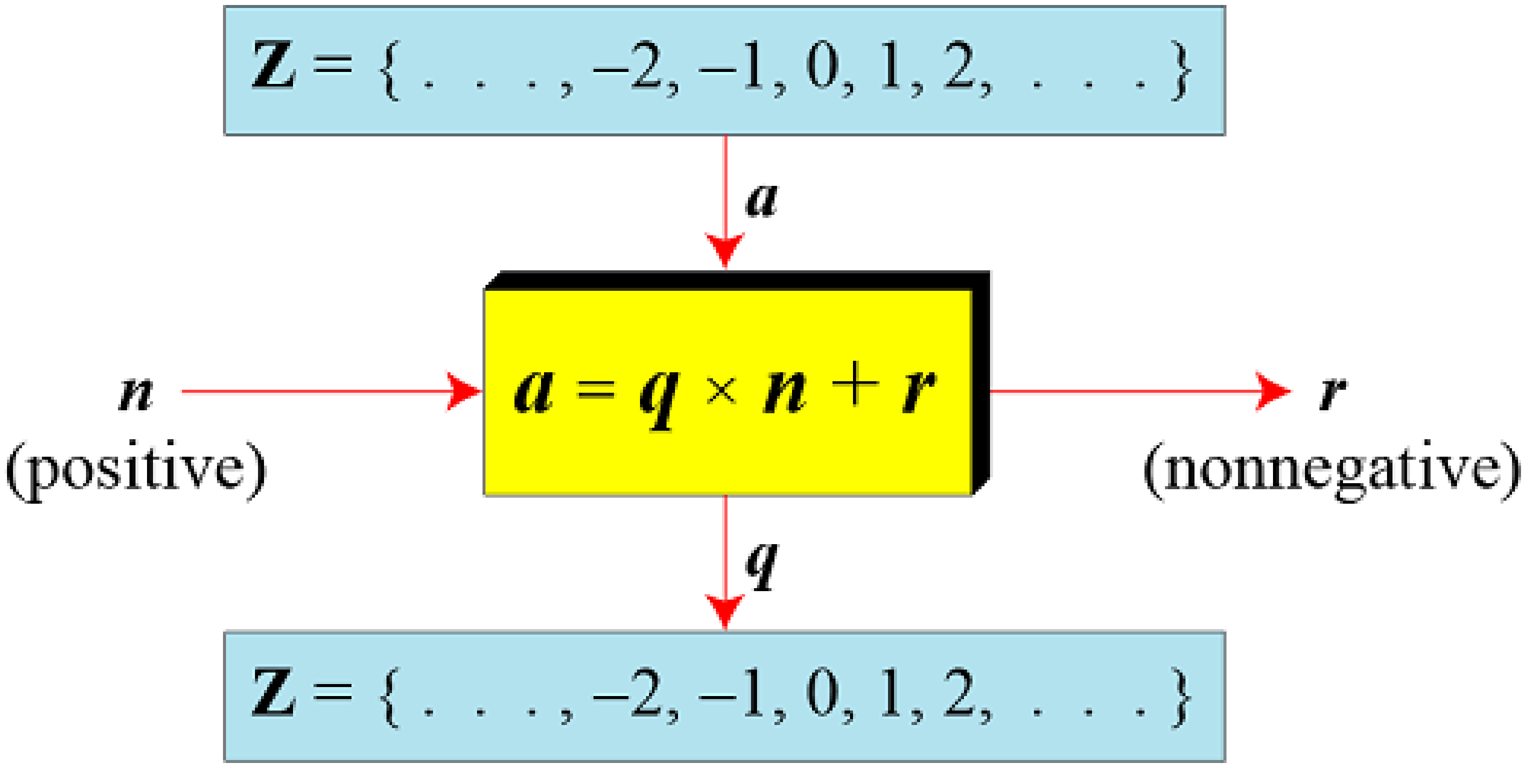
Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm.

Example #2



Finding the quotient and the remainder

Integer Division



Division algorithm for integers

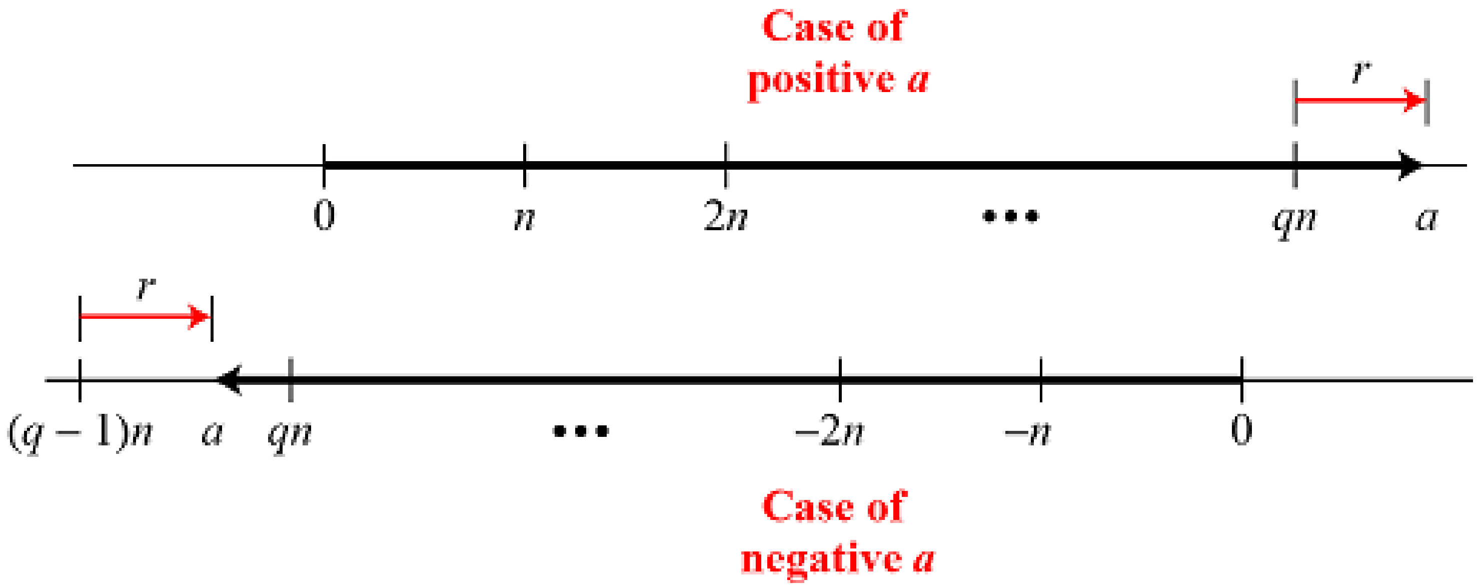
Integer Division

- 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.

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

Integer Division

- Graph of division algorithm



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, $n \mid a$
- If the remainder is not zero, $n \nmid a$

Example #3

a. The integer 4 divides the integer 32 because $\mathbf{32} = 8 \times \mathbf{4}$. We show this as $4|32$.

b. The number 8 does not divide the number 42 because $\mathbf{42} = 5 \times \mathbf{8} + 2$. There is a remainder, the number 2, in the equation. We show this as $8 \nmid 42$.

Divisibility

- Properties

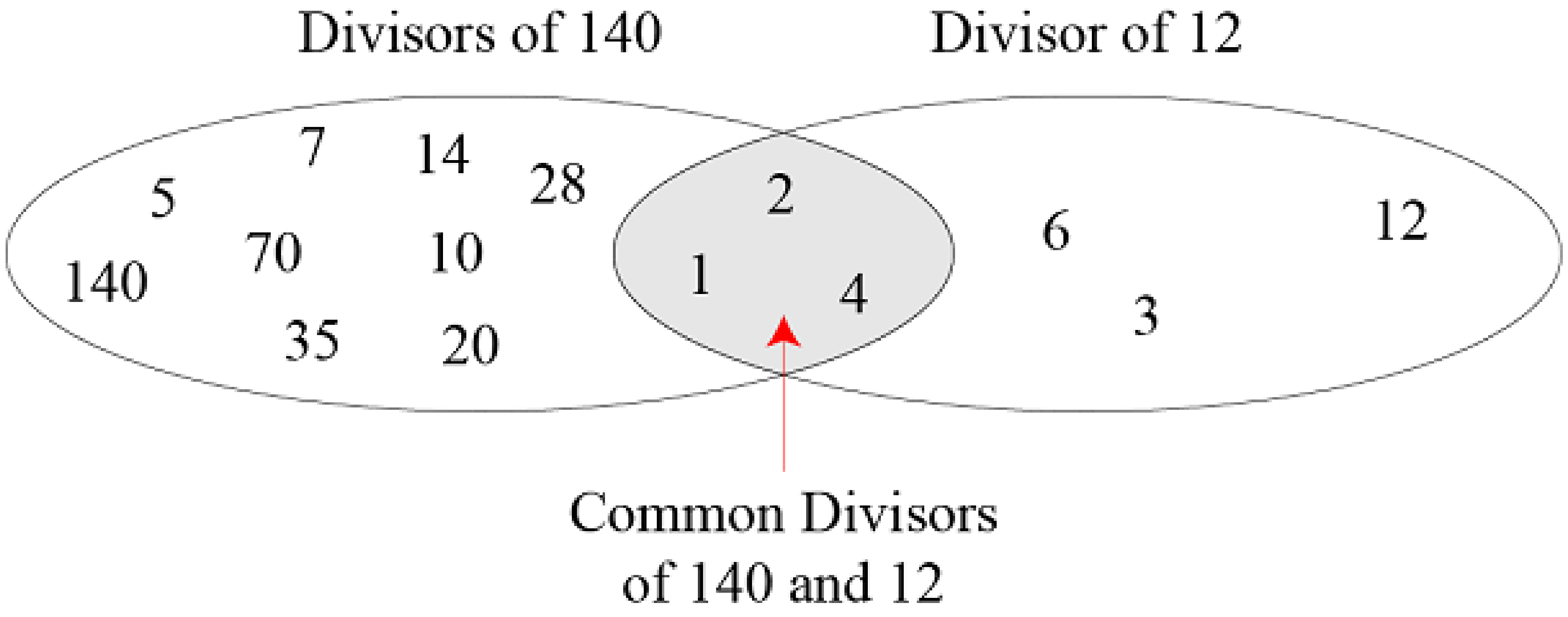
Property 1: if $a|1$, then $a = \pm 1$.

Property 2: if $a|b$ and $b|a$, then $a = \pm b$.

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

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

Divisibility



Common divisors of two integers

Divisibility

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

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

Example #4

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

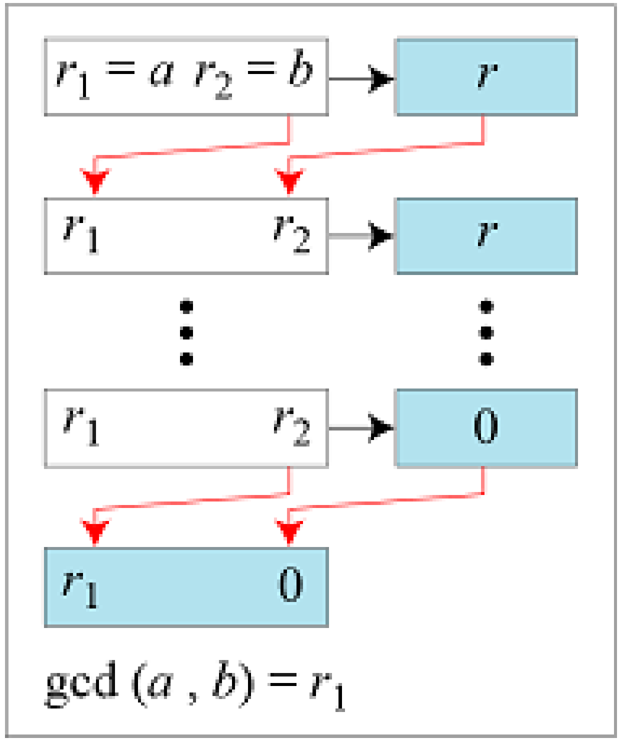
gcd (4, 2) = gcd (2, 0)...........by fact 2

gcd (2, 0) = 2.......................by fact 1

Hence, Answer = 2

Divisibility

Euclidean Algorithm



a. Process

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

while $(r_2 > 0)$

{

$\quad q \leftarrow r_1 / r_2;$

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

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

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

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

Divisibility

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	

Example #5

Answer: gcd (2740, 1760) = 20.

Divisibility

Class Exercise #1

Find the greatest common divisor of 25 and 60.

Divisibility

- **Extended Euclidean Algorithm**

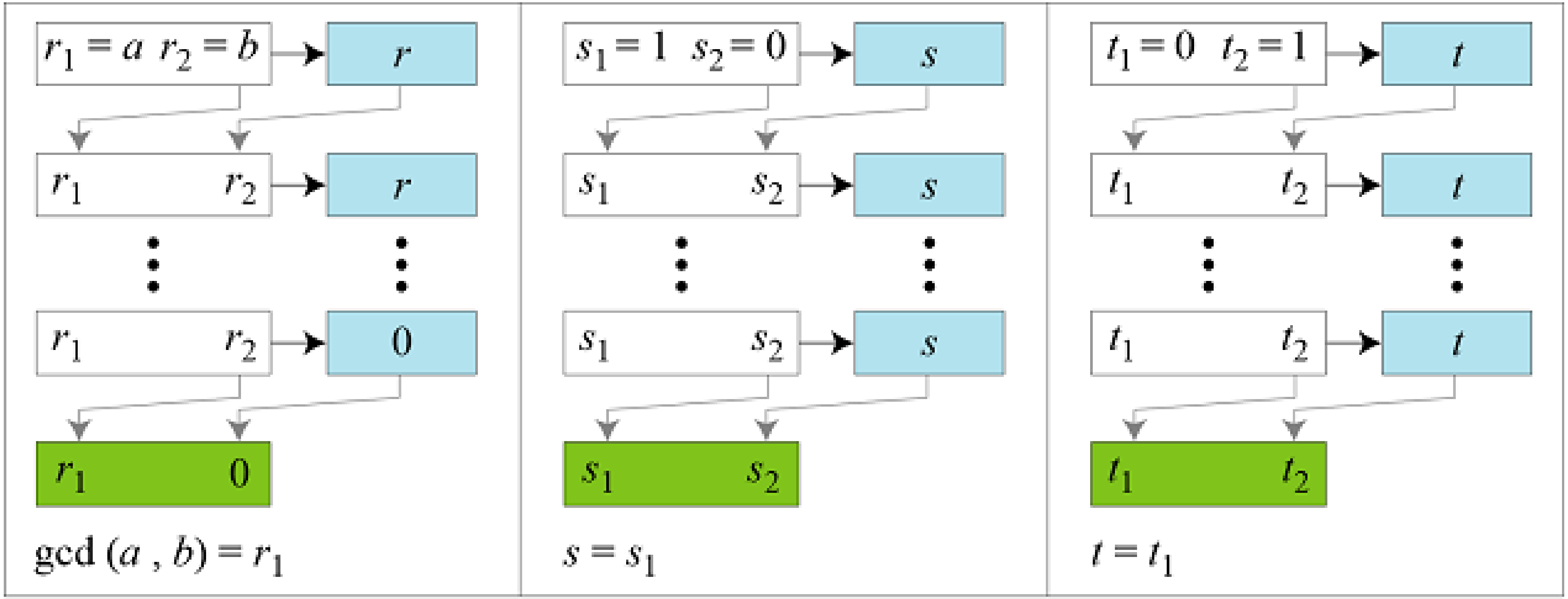
  Given two integers *a* and *b*, we often need to find other two integers, *s* and *t*, such that

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

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

Divisibility

Extended Euclidean algorithm, part a



a. Process

Divisibility

Extended Euclidean algorithm, part b

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

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

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

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

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

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

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 $d \mid c$, the equation has infinite number of solutions : one of them is particular and the rest are general**

Linear Diophantine Equations(cont.)

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

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

$21x + 14y = 35.$

Linear Diophantine Equations(cont.)

- d = gcd (21, 14) = 7.
- Since 7| 35, the equation has an infinite number of solutions.
- We can divide both sides by 7 to find the equation 3x + 2y = 5.
- Using the extended Euclidean algorithm, we find s and t such as 3s + 2t = 1. We have s = 1 and t = −1.

Particular: $x_0 = 5 \times 1 = 5$	and $y_0 = 5 \times (-1) = -5$	since 35/7 = 5
General: $x = 5 + k \times 2$	and $y = -5 - k \times 3$	where k is an integer

Therefore, the solutions are (5, −5), (7, −8), (9, −11), . . . We can easily test that each of these solutions satisfies the original equation.

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

Linear Diophantine Equations(cont.)

$d = \gcd(20, 5) = 5$ and $5 \mid 100$, infinite number of solutions,

$$4s + t = 1.$$

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

$$(0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0).$$

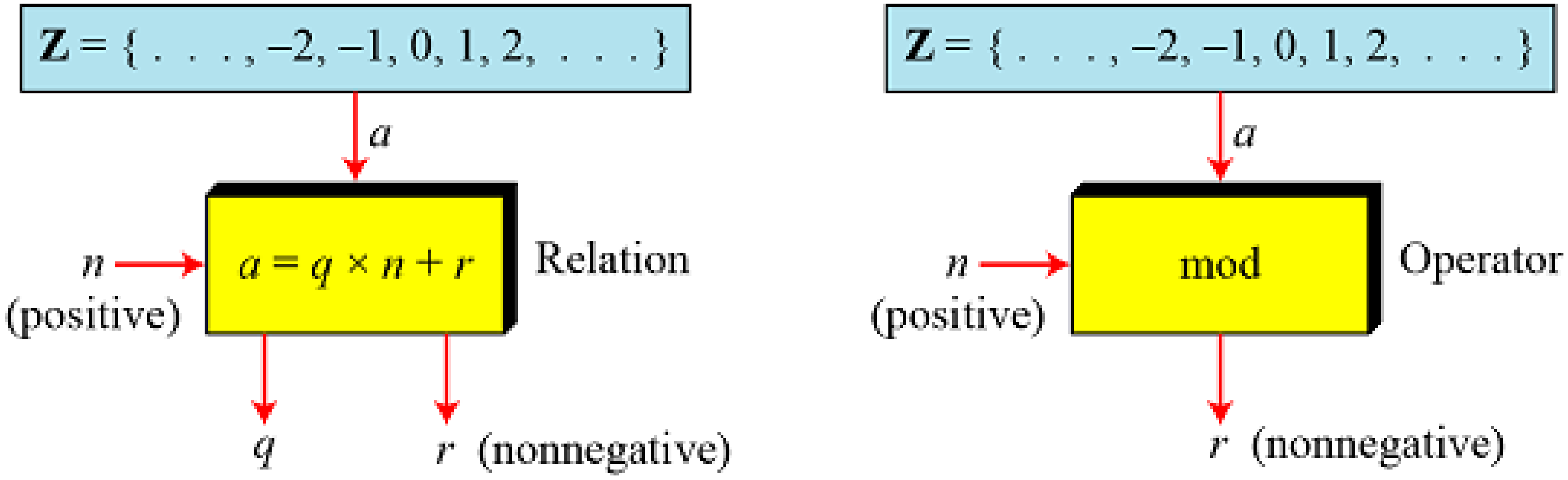
Modular Arithmetic

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.
- We use modular arithmetic in our daily life;
  - for example, we use a clock to measure time.
  - Our clock system uses modulo 12 arithmetic. However, instead of a 0 we use the number 12

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
- 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

- The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.

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

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

Some Z_n sets

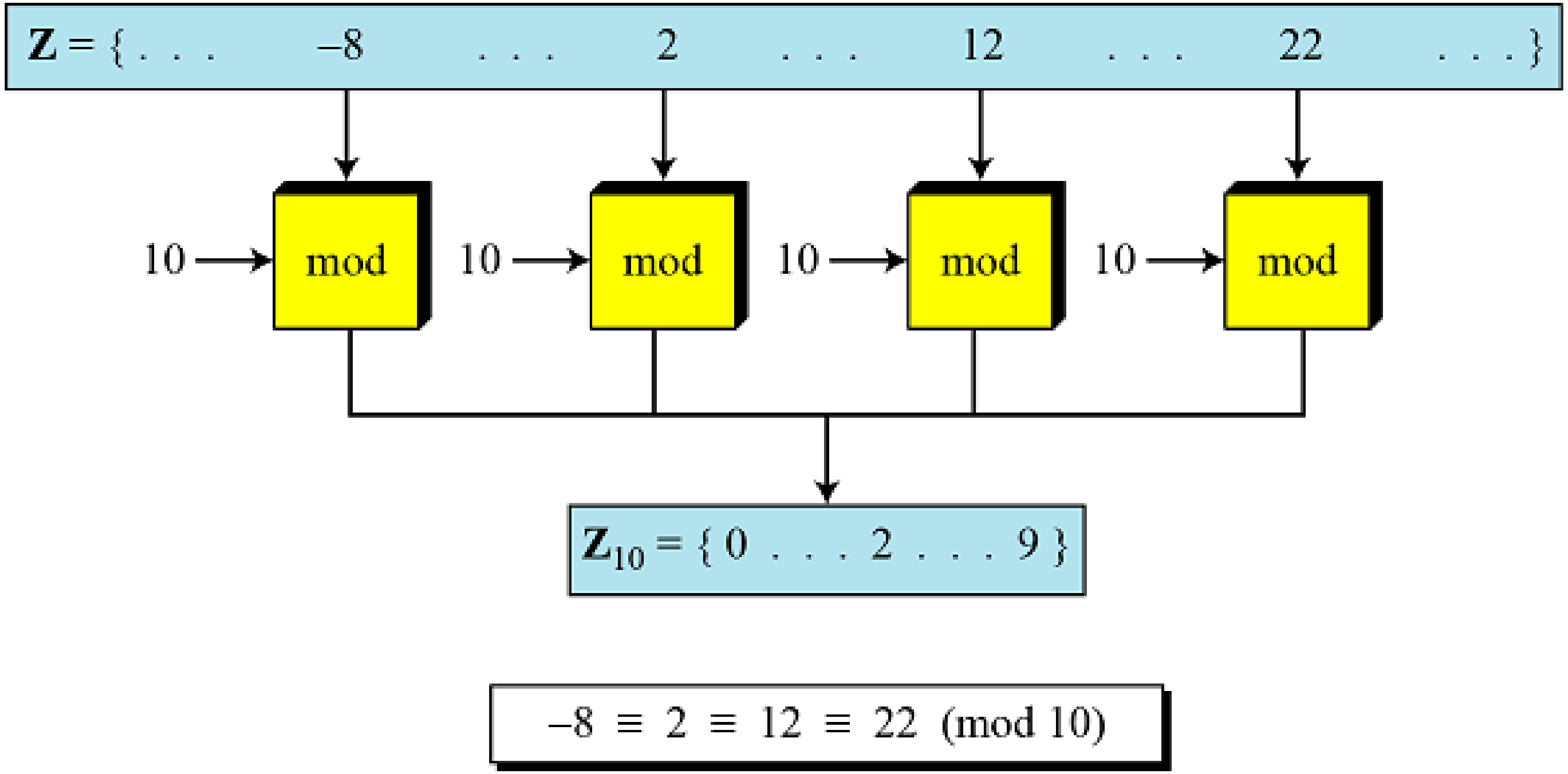
Congruence

- To show that two integers are congruent, we use the congruence operator (≡).
- For example, we write:

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

$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

Congruence



Congruence Relationship

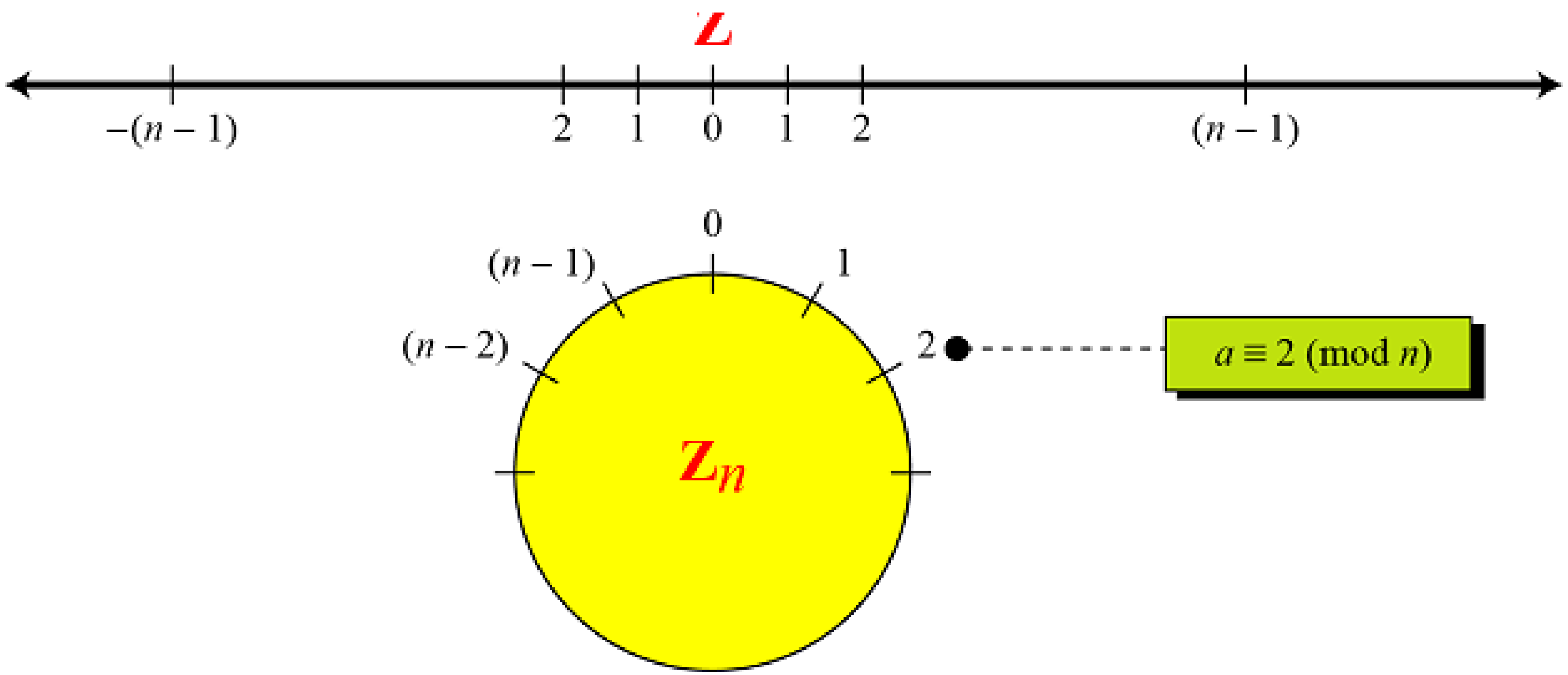
Congruence

- Residue Classes
  - A residue class [a] or $[a]_n$ is the set of integers congruent modulo n.
  - It is the set of all integers such that x=a(mod)n
  - E.g. for n=5, we have five sets as shown below:

$$
\begin{aligned}
[0] &= \{\ldots, -15, \ -10, \ -5, 0, \ 5, 10, 15, \ldots\} \\
[1] &= \{\ldots, -14, \ -9, \ -4, 1, \ 6, 11, 16, \ldots\} \\
[2] &= \{\ldots, -13, \ -8, \ -3, 2, \ 7, 12, 17, \ldots\} \\
[3] &= \{\ldots, -12, \ -7, \ -5, 3, \ 8, 13, 18, \ldots\} \\
[4] &= \{\ldots, -11, \ -6, \ -1, 4, \ 9, 14, 19, \ldots\}
\end{aligned}
$$

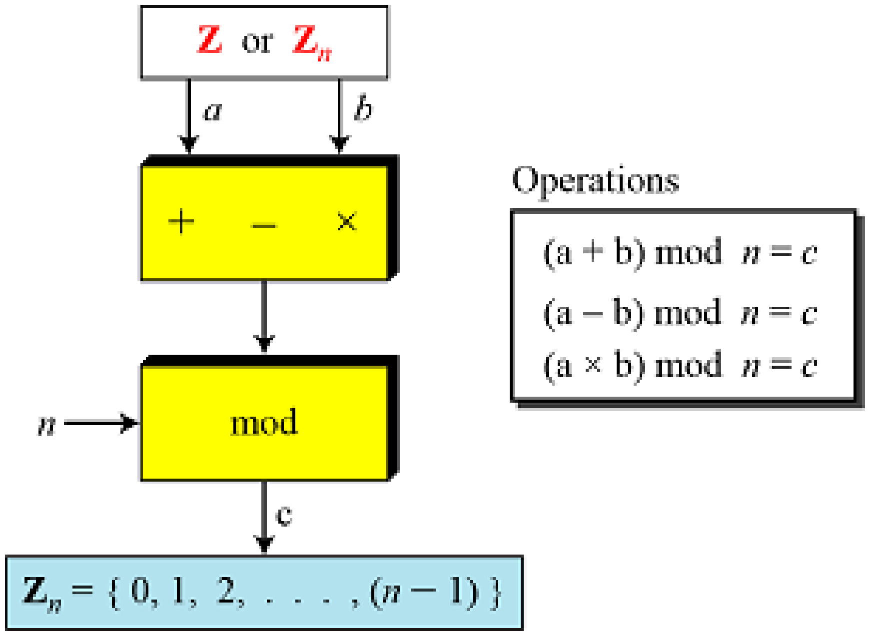
Congruence

- Comparison of Z and Z_n using graphs



Operation in Z_n

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



Operation in Z_n

- 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}.
- Solution

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

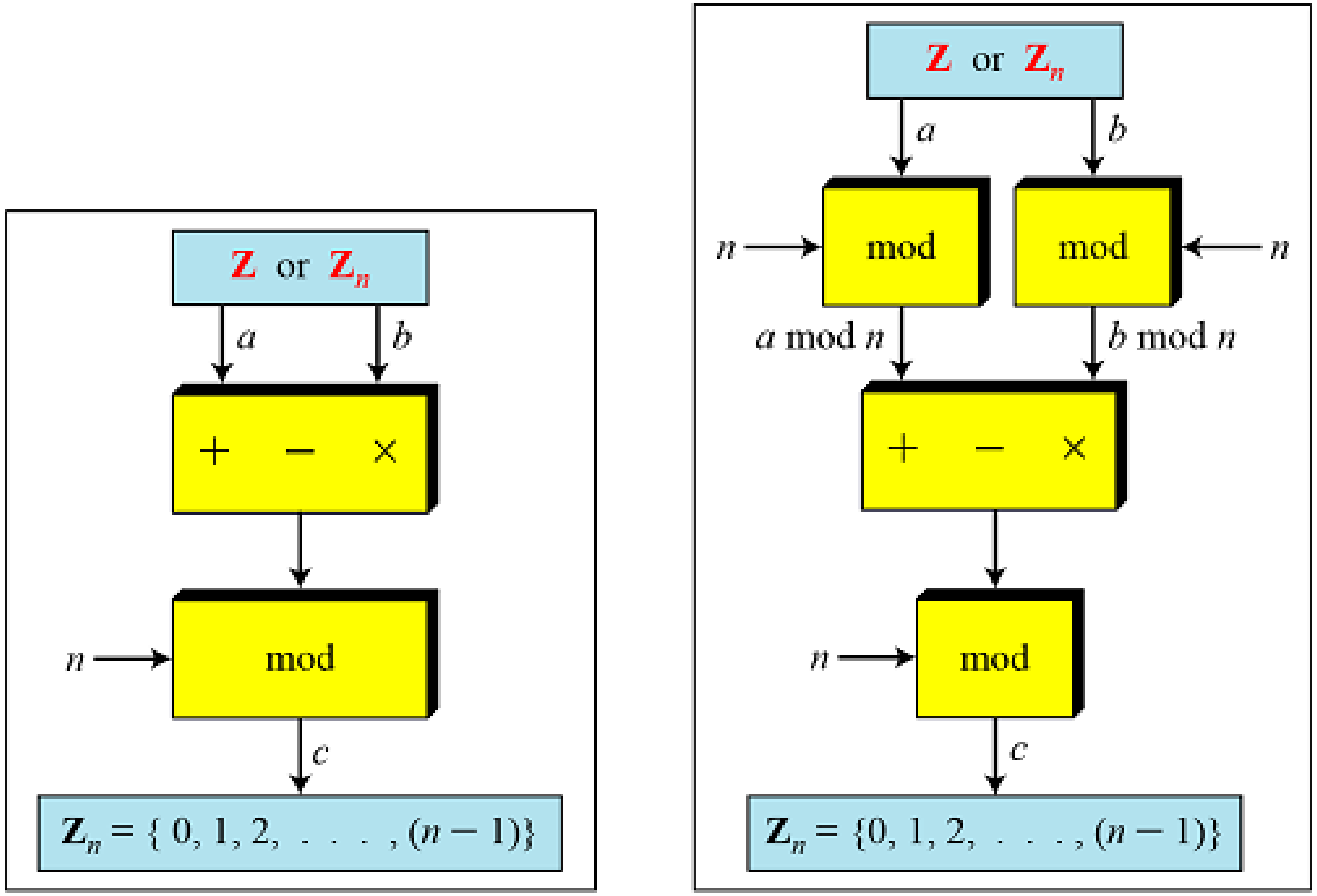
Operation in Z_n

- 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}.
- Solution
  a. Add 17 to 27 in Z_{14}: (17+27)mod 14 = 2
  - Subtract 43 from 12 in Z_{13} : (12-43)mod 13 = 8
  - 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.)



a. Original process

b. Applying properties

Operation in Z_n(cont.)

- The following shows the application of the above properties:

  1. $(1{,}723{,}345 + 2{,}124{,}945) \bmod 11 = (8 + 9) \bmod 11 = 6$
  2. $(1{,}723{,}345 - 2{,}124{,}945) \bmod 11 = (8 - 9) \bmod 11 = 10$
  3. $(1{,}723{,}345 \times 2{,}124{,}945) \bmod 11 = (8 \times 9) \bmod 11 = 6$

Operation in Z_n(cont.)

- In arithmetic, we often need to find the remainder of powers of 10 when divided by an integer.

$10^n \bmod x = (10 \bmod x)^n$ Applying the third property n times.

$$10 \bmod 3 = 1 \quad \rightarrow \quad 10^n \bmod 3 = (10 \bmod 3)^n = 1$$
$$10 \bmod 9 = 1 \quad \rightarrow \quad 10^n \bmod 9 = (10 \bmod 9)^n = 1$$
$$10 \bmod 7 = 3 \quad \rightarrow \quad 10^n \bmod 7 = (10 \bmod 7)^n = 3^n \bmod 7$$

Inverses

- When we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation.
- We are normally looking for an additive inverse (relative to an addition operation) or a multiplicative inverse (relative to a multiplication operation).

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 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

- 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

- Find all multiplicative inverse pairs in Z_{11}.
- Solution
  - We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), and (10, 10).