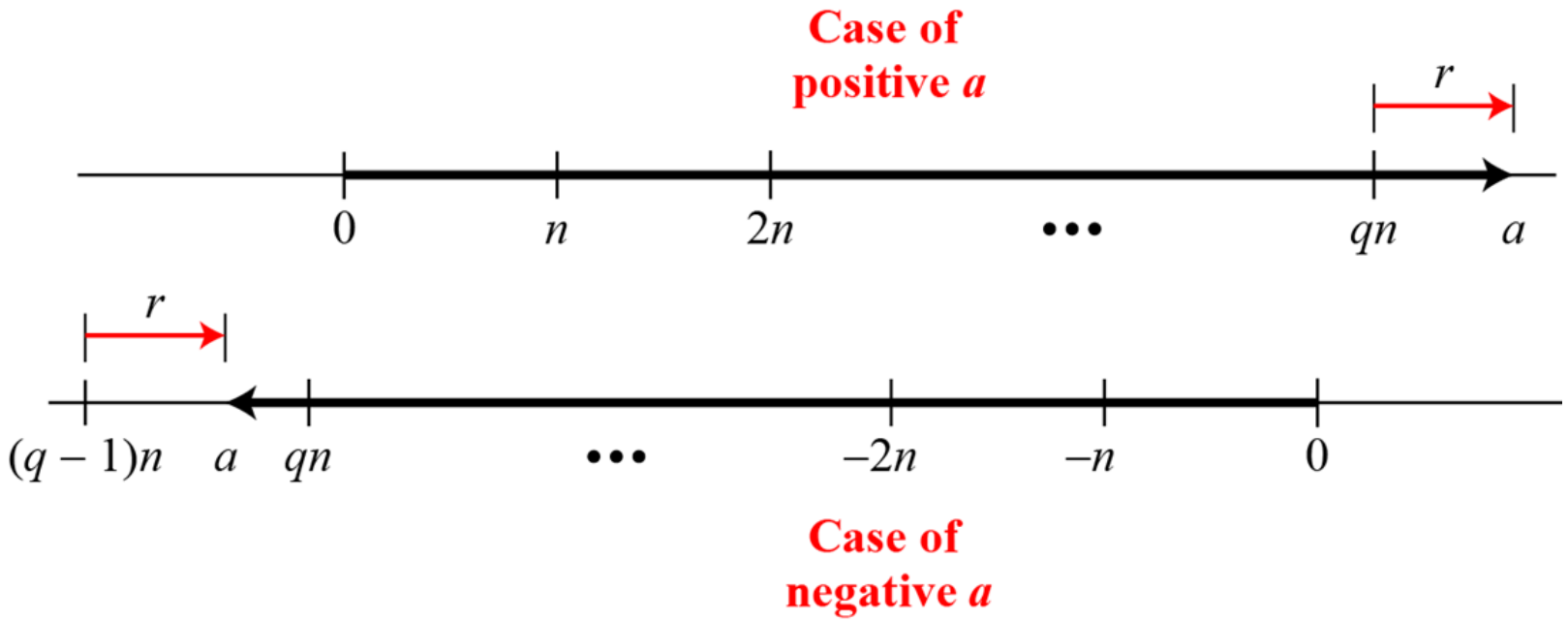
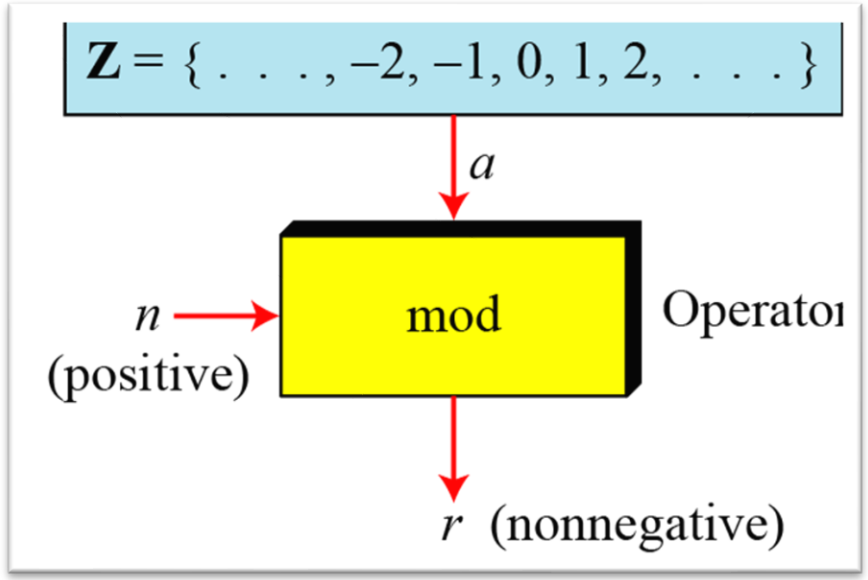
Mathematics of Cryptography

Modulo Operator

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





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: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Modulo Operator

Example

Find the result of the following operations:

a. 27 mod 5
b. 36 mod 12
c. −18 mod 14
d. −7 mod 10

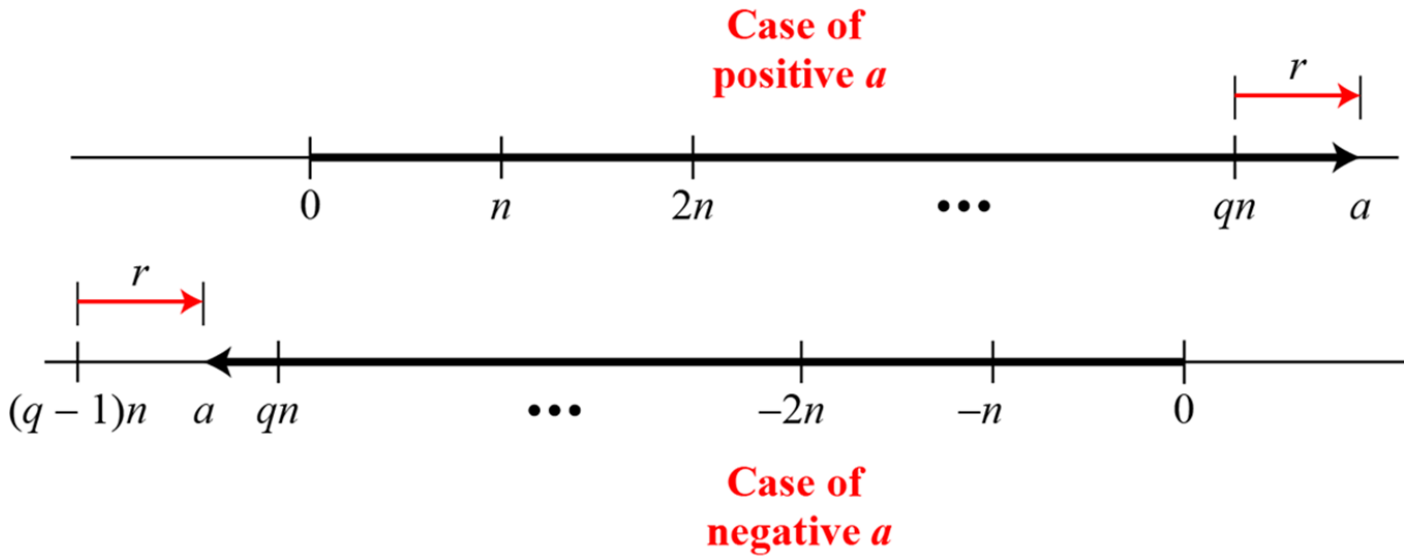
Solution

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.



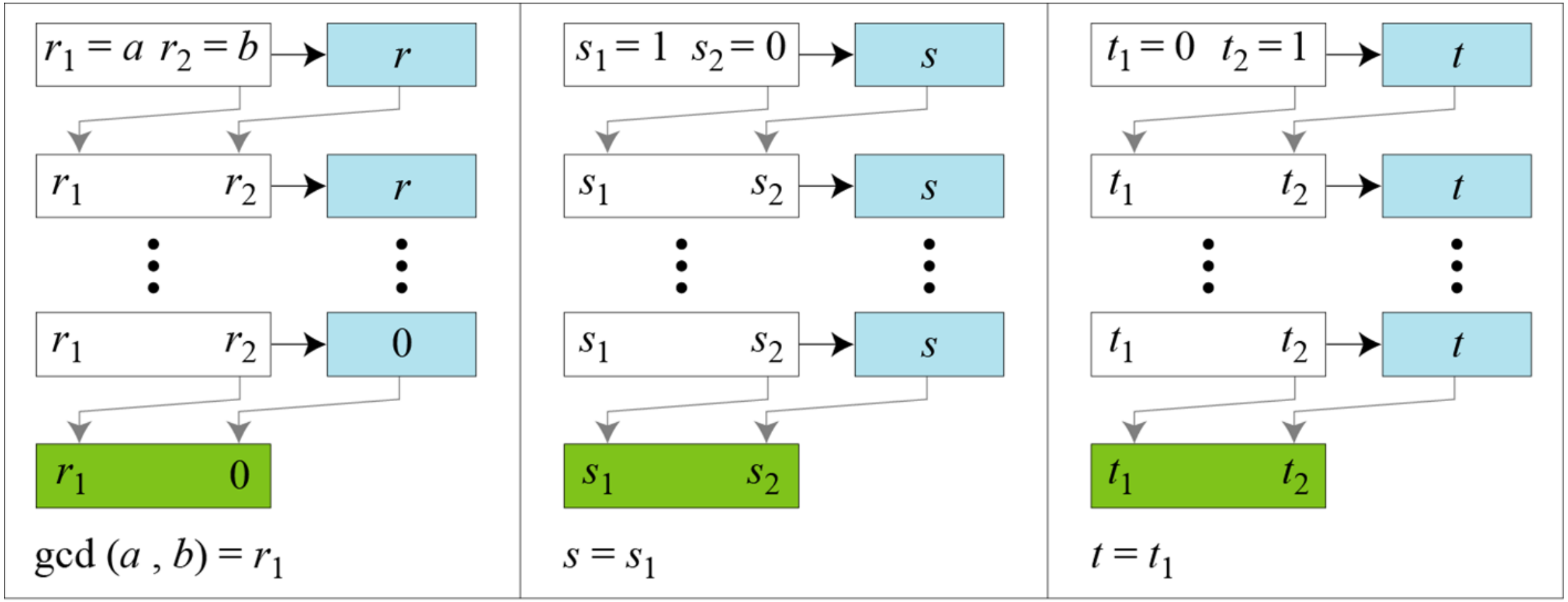
Extended Euclidean Algorithm

- 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.

Extended Euclidean Algorithm



Extended Euclidean Algorithm

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

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

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	

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.

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

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

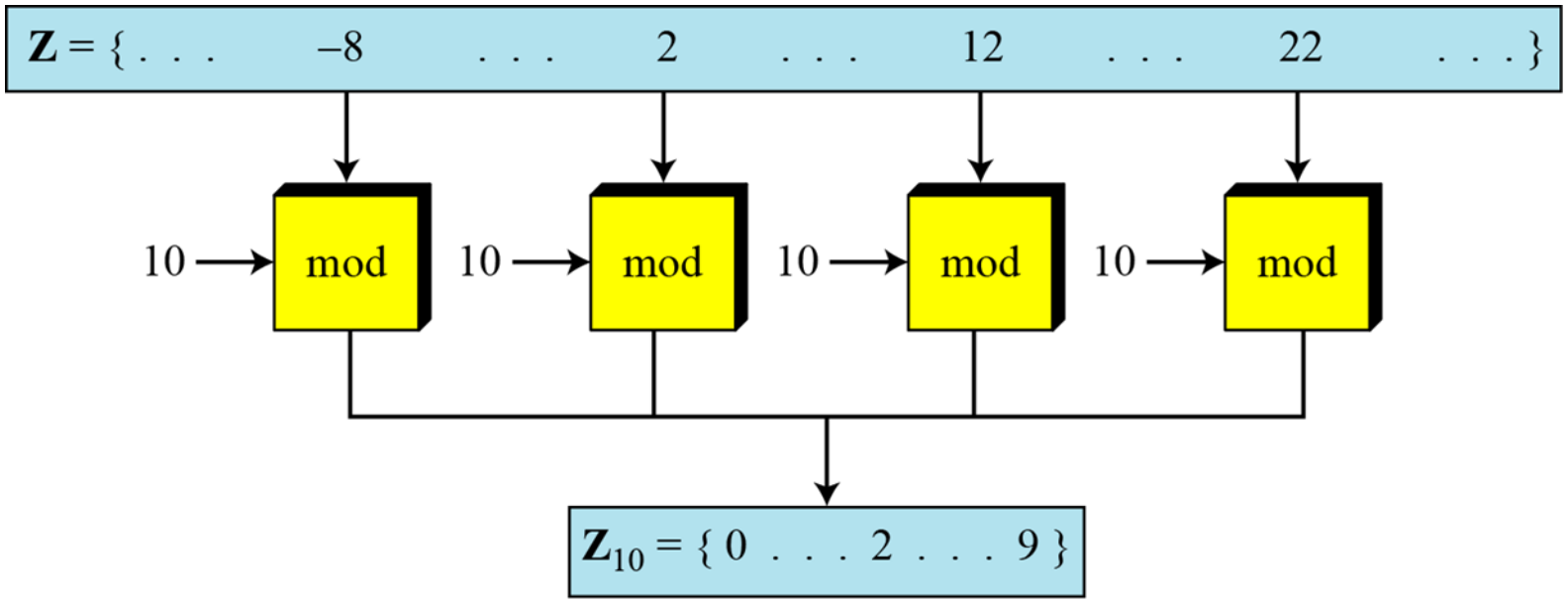
Some Z_n sets

Congruence

To show that two integers are congruent, we use the congruence operator (≡)

Example

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

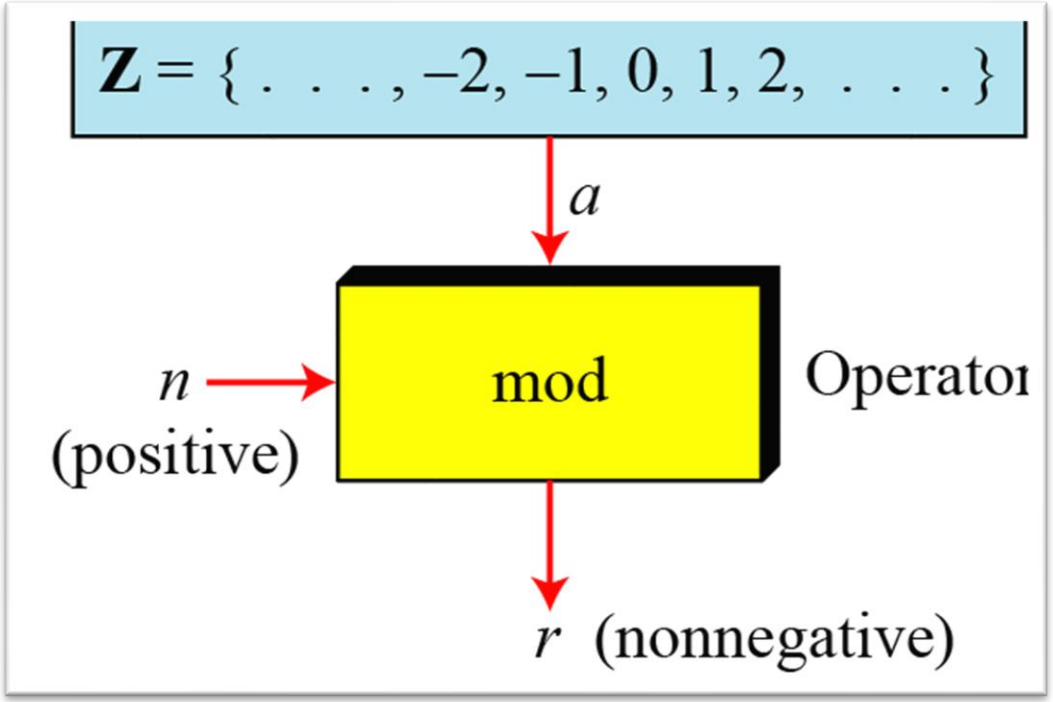


$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

Modulo Operator

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



- Let a,b,c,n be integers with n≠0

(1) a≡0 (mod n) iff n|a

(2) a≡a (mod n)

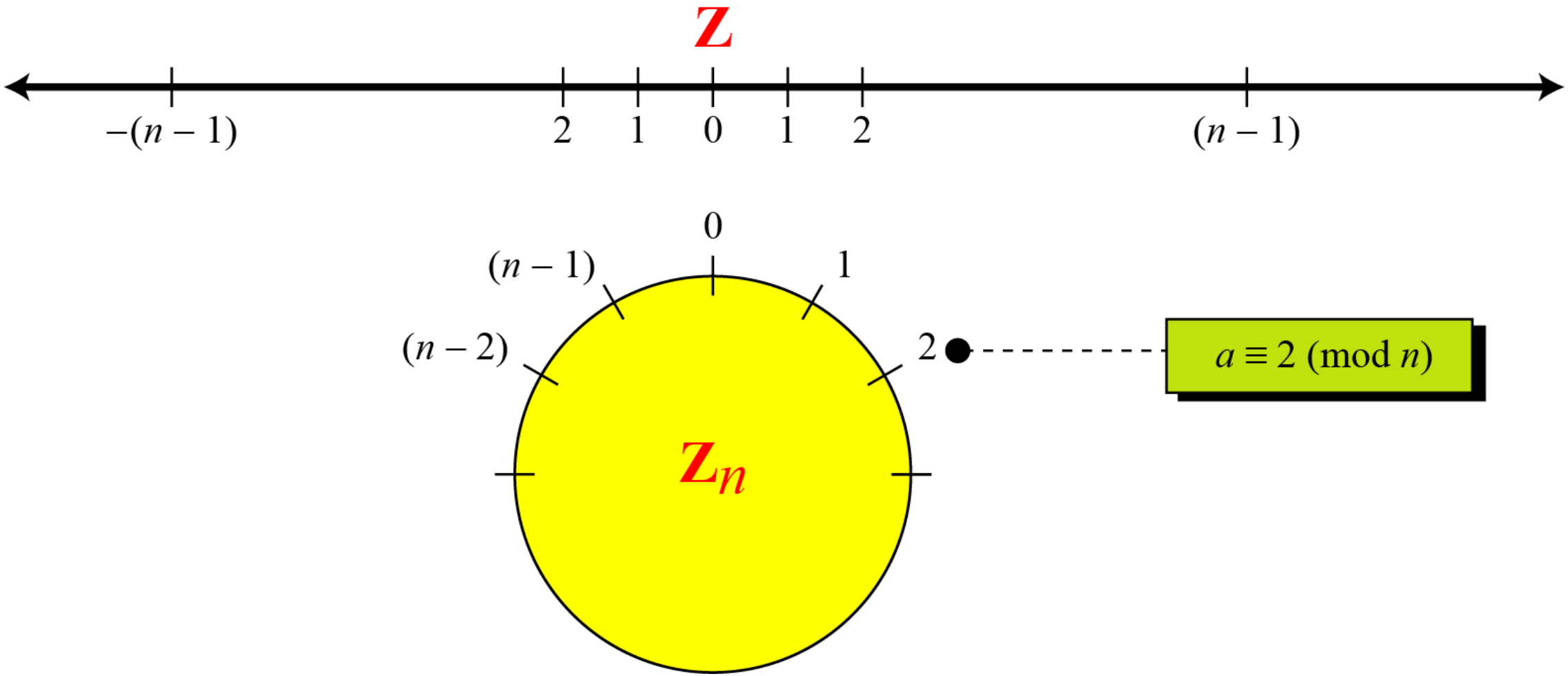
(3) a≡b (mod n) iff b≡a (mod n)

(4) a≡b and b≡c (mod n) → a≡c (mod n)

(5) a≡b and c≡d (mod n) → a+c≡b+d,
a−c≡b−d, ac≡bd (mod n)

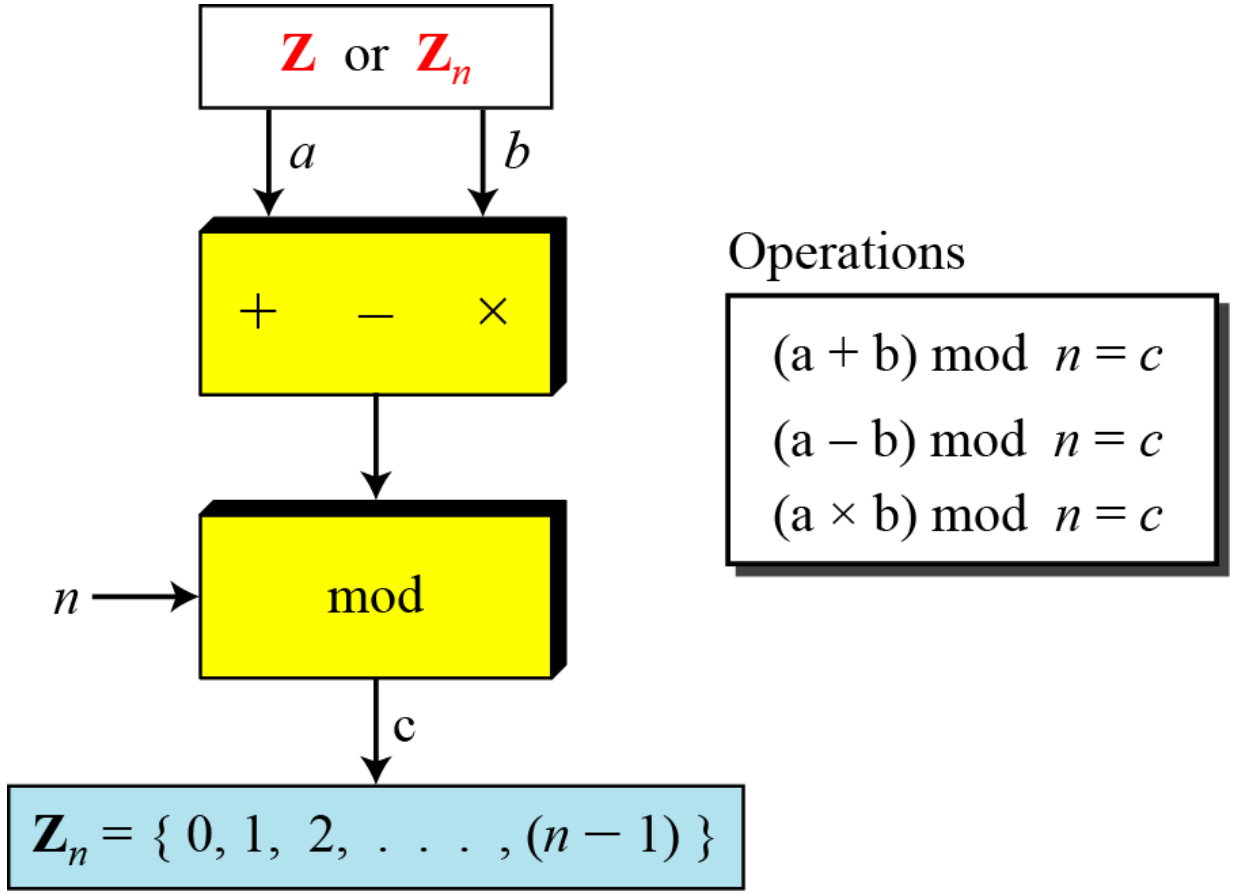
(6) ab≡ac (mod n) with n≠0, and gcd(a,n)=1, then b≡c (mod n)

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 Zn. The result may need to be mapped to Zn using the mod operator.



Binary operations in Z_n

Operation in Z_n

Example

Perform the following operations (the inputs come from Zn):

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

$$(14 + 7) \bmod 15$$
$$(7 - 11) \bmod 13$$
$$(7 \times 11) \bmod 20$$

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

Operation in Z_n

Example 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

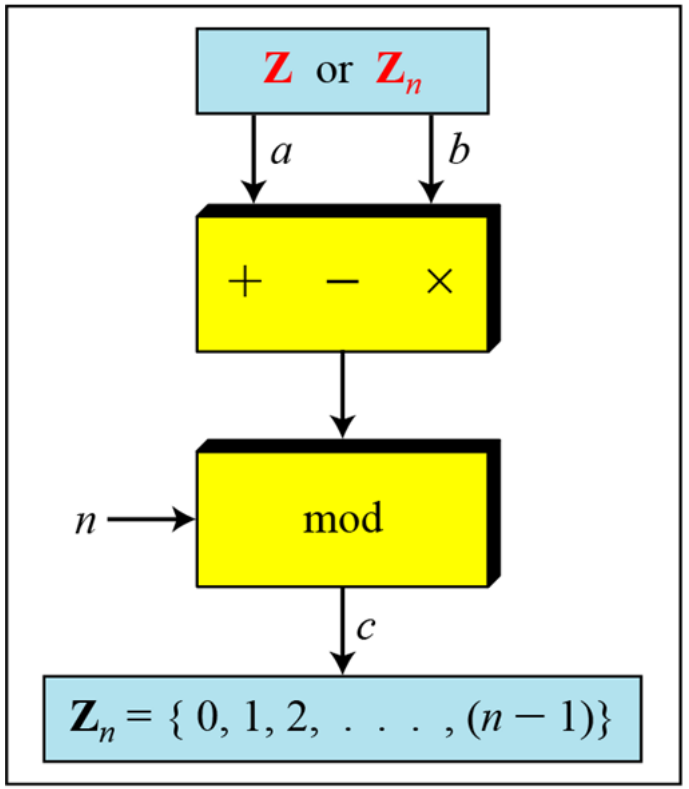
Additive Inverse

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

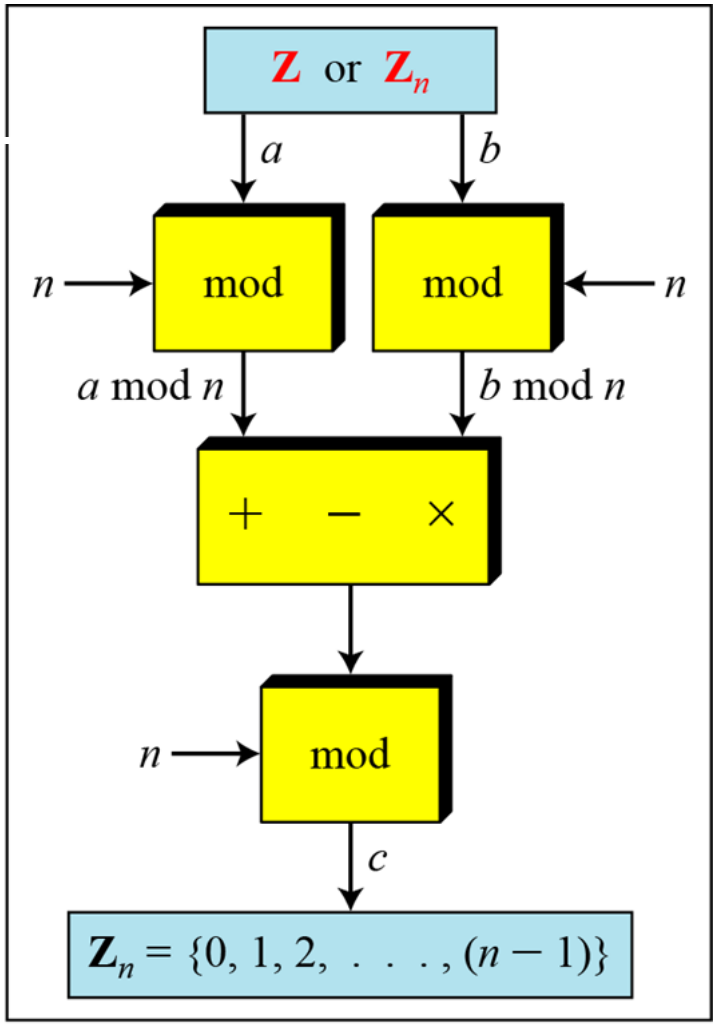
Multiplicative Inverse

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

$$10^n \bmod x = (10 \bmod x)^n$$



a. Original process



b. Applying properties

$$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$$
$$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$$
$$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$$

Extended Euclidean Algorithm

Example 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.

Zn and Zn* sets

Use Z_n when additive inverses are needed

Use Z_n^* when multiplicative inverses are needed

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

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

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

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

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

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

MATRICES

- A matrix of size $l \times m$

Matrix **A**:

$$\begin{array}{c} \\ l \text{ rows} \end{array} \overbrace{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix}}^{m \text{ columns}}$$

- Examples of matrices

$$\begin{bmatrix} 2 & 1 & 5 & 11 \end{bmatrix}$$

Row matrix

$$\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}$$

Column matrix

$$\begin{bmatrix} 23 & 14 & 56 \\ 12 & 21 & 18 \\ 10 & 8 & 31 \end{bmatrix}$$

Square matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

0

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

I

Residue Matrices

Cryptography uses residue matrices: matrices where all elements are in Z_n. A residue matrix has a multiplicative inverse if gcd (det(A), n) = 1.

Example

A residue matrix and its multiplicative inverse

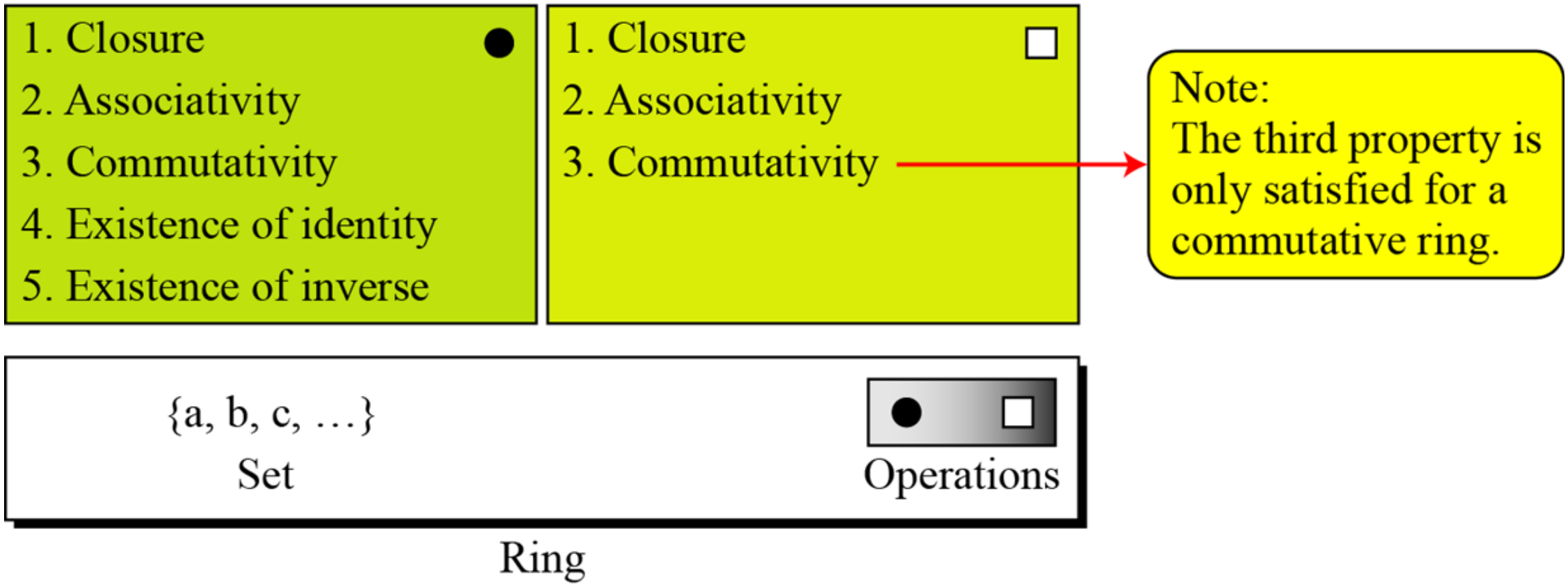
$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$\det(\mathbf{A}) = 21 \qquad \det(\mathbf{A}^{-1}) = 5$$

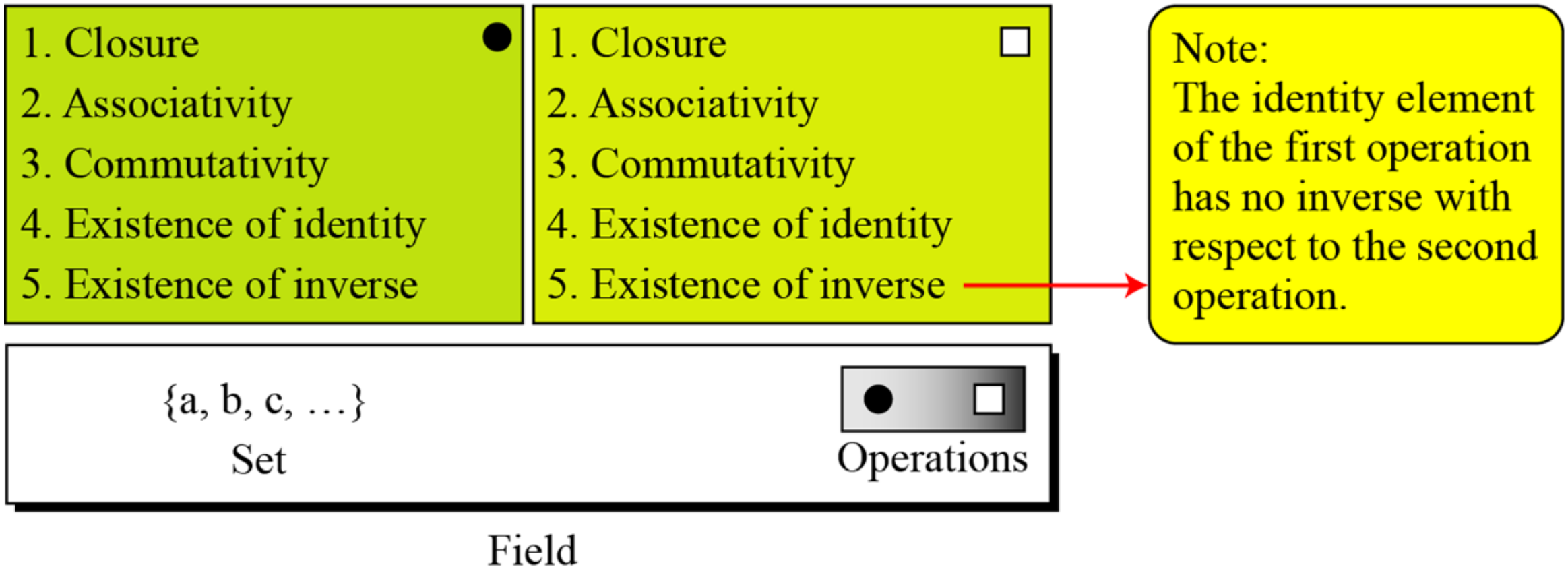
Note

- Multiplicative inverses are only defined for square matrices.

Ring


1. Closure
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse
1. Closure
2. Associativity
3. Commutativity
Note:
The third property is only satisfied for a commutative ring.
{a, b, c, …}
Set
Operations
Ring

Field


1. Closure
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse
1. Closure
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse
Note:
The identity element of the first operation has no inverse with respect to the second operation.
{a, b, c, …}
Set
Operations
Field

Finite Fields

A Galois field, GF(p^n), is a finite field with p^n elements.

Galois showed that for a field to be finite, the number of elements should be p^n, where p is a prime and n is a positive integer.

Let us define a GF(2^2) field in which the set has four 2-bit words: {00, 01, 10, 11}. We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied.

Addition

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

Multiplication

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

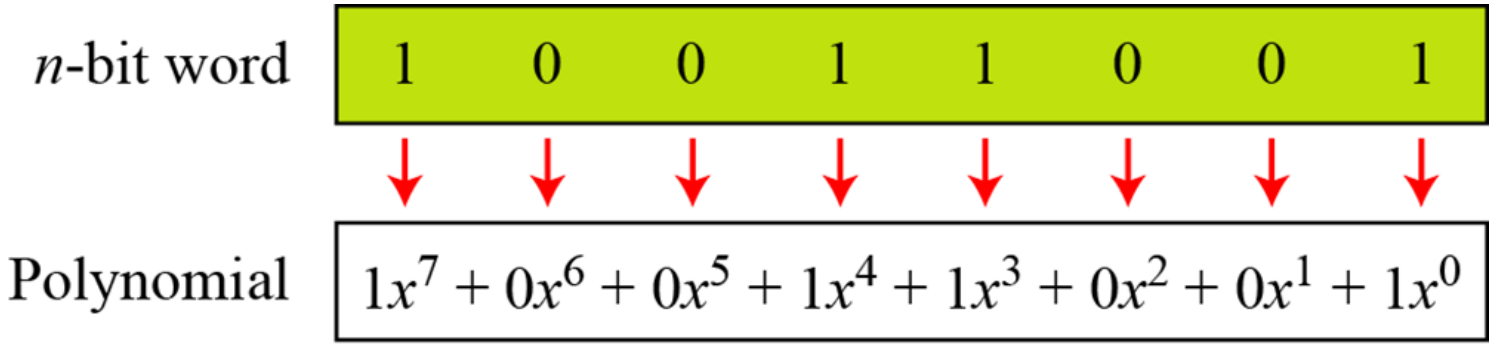
Polynomials

- A polynomial of degree $n - 1$ is an expression of the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

- where x^i is called the ith term and a_i is called coefficient of the *i*th term.

Representation of an 8-bit word by a polynomial



First simplification $1x^7 + 1x^4 + 1x^3 + 1x^0$

Second simplification $x^7 + x^4 + x^3 + 1$

Multiplication of $GF(2^n)$

Example

- $(X^7+ X^6 + X^3 + X + 1)\,(X) = ?\ (\mathrm{mod}\ X^8+ X^4 + X^3 + X + 1)$
- 11001011 $b_7=1$
- Left shift one bit, we have

  $b_6\, b_5\, b_4\, b_3 b_2\, b_1\, b_0 0 = 10010110$

- $?=110010110 + 100011011 = 10001101$

  $=X^7+X^3+X^2+1$

Extended Euclidean Algorithm

Example In GF(2^8), find the inverse of (x^5) modulo ($x^8 + x^4 + x^3 + x + 1$)

Solution

Euclidean algorithm

q	r_1	r_2	r	t_1	t_2	t
(x^3)	$(x^8 + x^4 + x^3 + x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	(0)	(1)	(x^3)
$(x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$
(x)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$	$(x^5 + x^4 + x^3 + x)$
$(x^3 + x^2 + 1)$	$(x^3 + x^2 + 1)$	(1)	(0)	$(x^4 + x^3 + 1)$	$(x^5 + x^4 + x^3 + x)$	(0)
	(1)	(0)		$(x^5 + x^4 + x^3 + x)$	(0)	

- The answer is ($x^5 + x^4 + x^3 + x$) as shown in above Table

Prime Numbers

- ***Prime Number***

An integer p>1 that is divisible only by 1 and itself is called a prime number, otherwise it is called composite

- ***Number of Primes***

Let π(x) be the number of primes less than x, then π(x) ≈x/ln(x) as x→∞

$$[n / (\ln n)] \quad < \quad \pi(n) \quad < \quad [n/(\ln n - 1.08366)]$$

$\pi(1) = 0 \quad \pi(2) = 1 \quad \pi(3) = 2 \quad \pi(10) = 4 \quad \pi(20) = 8 \quad \pi(50) = 15 \quad \pi(100) = 25$

Checking for Primeness

Given a number **n**, how can we determine if n is a prime?

The answer is that we need to see if the number is divisible by all primes less than $\sqrt{n}$

Example Is 97 a prime?

Solution The floor of $\sqrt{97} = 9$. The primes less than 9 are 2, 3, 5, and 7.

We need to see if 97 is divisible by any of these numbers.

It is not, so 97 is a prime.

Checking for Primeness

Sieve of Eratosthenes

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

The Greek mathematician Eratosthenes devised a method to find all primes less than n. The method is called the **sieve of Eratosthenes.** Suppose we want to find all prime less than 100. We write down all the numbers between 2 and 100. Because $\sqrt{100} = 10$, we need to see if any number less than 100 is divisible by 2, 3, 5, and 7. Table 9.1 shows the result.

Euler's Phi-Function

Euler's phi-function, ϕ (n), which is sometimes called the

Euler's totient function plays a very important role in cryptography.

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Euler's Phi-Function

We can combine the above four rules to find the value of $\phi(n)$. For example, if n can be factored as

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

then we combine the third and the fourth rule to find

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})$$

Note

The difficulty of finding $\phi(n)$ depends on the difficulty of finding the factorization of *n*.

Extended Euclidean Algorithm

Example What is the value of $\phi(13)$?

Solution

- Is 13 a prime? =>Yes/No , why?
- $\phi(13) = (13 - 1) = 12$

Example What is the value of $\phi(10)$?

Solution

We can use the third rule:
$\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes

Extended Euclidean Algorithm

Example What is the value of $\phi(240)$?

Solution We can write $240 = 2^4 \times 3^1 \times 5^1$.

Then $\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$

Example Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Solution No.

The third rule applies when *m* and *n* are relatively prime.

Here $49 = 7^2$. We need to use the fourth rule: $\phi(49) = 7^2 - 7^1 = 42$.

Extended Euclidean Algorithm

Example What is the number of elements in Z_{14}^*?

Solution The answer is $\phi(14) = \phi(7) \times \phi(2) = 6 \times 1 = 6$

The members are 1, 3, 5, 9, 11, and 13.

Note

Interesting point: If $n > 2$, the value of $\phi(n)$ is even.

Fermat's Little Theorem

- ***First Version***

$$a^{p-1} \equiv 1 \bmod p$$

Example Find the result of $6^{10} \bmod 11$

Solution We have $6^{10} \bmod 11 = 1$
This is the first version of Fermat's little theorem where $p = 11$

- ***Second Version***

$$a^{p} \equiv a \bmod p$$

Example Find the result of $3^{12} \bmod 11$

Solution Here the exponent (12) and the modulus (11) are not the same. With substitution this can be solved using Fermat's little theorem.

$$3^{12} \bmod 11 = (3^{11} \times 3) \bmod 11 = (3^{11} \bmod 11)\ (3 \bmod 11) = (3 \times 3) \bmod 11 = 9$$

Fermat's Little Theorem

Multiplicative Inverses

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

Example The answers to multiplicative inverses modulo a prime can be found without using the extended Euclidean algorithm:

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$

Euler's Theorem

- ***First Version***

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

- ***Second Version***

$$a^{k \times \phi(n) + 1} \equiv a \pmod{n}$$

Example Find the result of $6^{24} \bmod 35$

Solution

We have $6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35 = 1$

Example Find the result of $20^{62} \bmod 77$

Solution

If we let $k = 1$ on the second version,
we have $20^{62} \bmod 77$
$= (20 \bmod 77)\ (20^{\phi(77)\ +\ 1} \bmod 77) \bmod 77$
$= (20)(20) \bmod 77 = 15$

Euler's Theorem

Multiplicative Inverses

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

Euler's theorem can be used to find multiplicative inverses modulo a composite

Example The answers to multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm if we know the factorization of the composite:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$

Exponentiation and Logarithm

Exponentiation: $y = a^x$ $\rightarrow$ **Logarithm:** $x = \log_a y$

Fast Exponentiation

$$y = a^{x_{n_b-1} \times 2^{n_b-1} + x_{n_b-2} \times 2^{n_b-2} + \cdots + x_1 \times 2^1 + x_0 \times 2^0}$$

in which x_i is 0 or 1

$$y = \boxed{a^{2^{n_b-1}} \text{ or } 1} \times \boxed{a^{2^{n_b-2}} \text{ or } 1} \times \cdots \times \boxed{a^2 \text{ or } 1} \times \boxed{a \text{ or } 1}$$

Example:

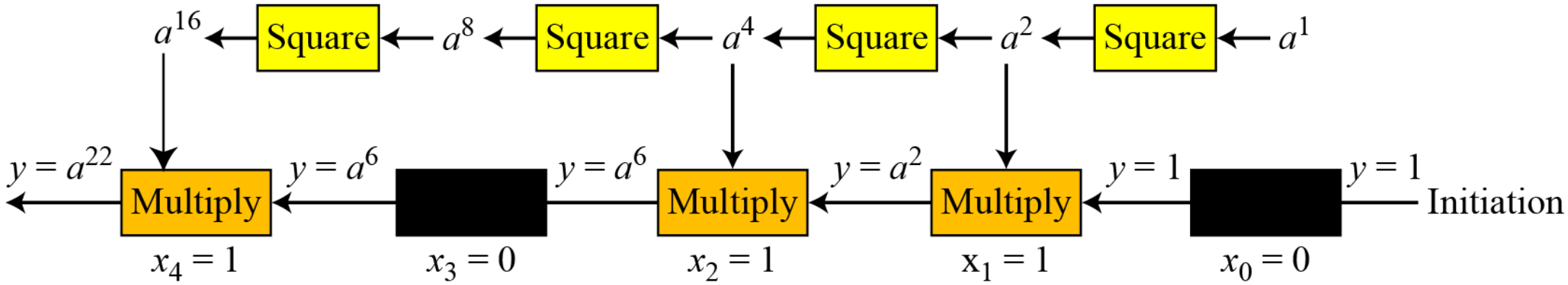
$$y = a^9 = a^{1001_2} = a^8 \times 1 \times 1 \times a$$

Square-and-multiply method

Example

Demonstration of calculation of a^{22} using square-and-multiply method

Solution

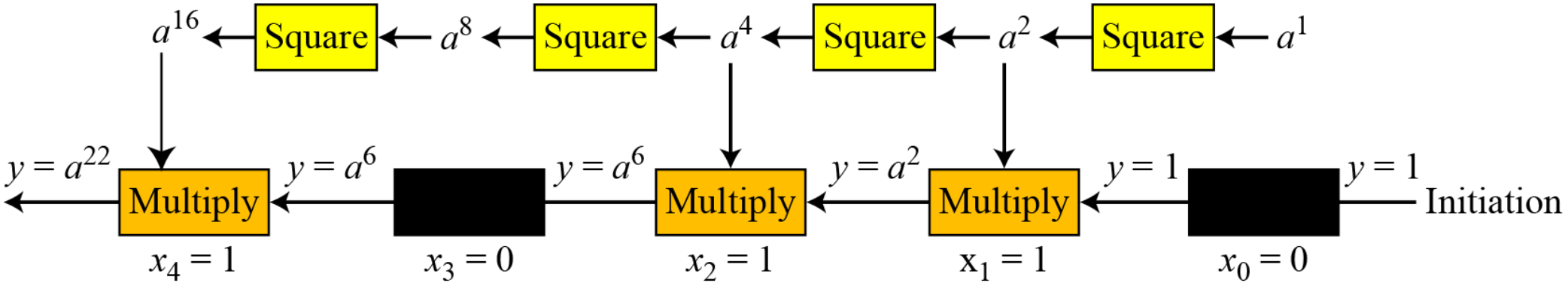


Process for calculating $y = a^x$ using square-and-multiply method (for simplicity, the modulus is not shown).

In this case, $x = 22 = (10110)2$ in binary. The exponent has five bits.

Square-and-multiply method

Demonstration of calculation of a^{22} using square-and-multiply method



Example

Calculation of ***17^{22} mod 21*** *using square-and-multiply method*

Solution

i	x_i	*Multiplication (Initialization: $y = 1$)*	*Squaring (Initialization: $a = 17$)*
0	0	$\rightarrow$	$a = 17^2 \bmod 21 = 16$
1	1	$y = 1 \times 16 \bmod 21 = 16$ $\rightarrow$	$a = 16^2 \bmod 21 = 4$
2	1	$y = 16 \times 4 \bmod 21 = 1$ $\rightarrow$	$a = 4^2 \bmod 21 = 16$
3	0	$\rightarrow$	$a = 16^2 \bmod 21 = 4$
4	1	$y = 1 \times 4 \bmod 21 = 4$ $\rightarrow$	

Order of the Group

What is the order of group $G = \langle Z_{21}^*, \times \rangle$?

$|G| = \phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$.

There are 12 elements in this group: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, and 20. All are relatively prime with 21.

Order of an Element

Problem Find the order of all elements in $G = \langle Z_{10}^*, \times \rangle$

Solution

This group has only $\phi(10) = 4$ elements: 1, 3, 7, 9. We can find the order of each element by trial and error.

a. $1^1 \equiv 1 \bmod (10) \rightarrow \text{ord}(1) = 1$

b. $3^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(3) = 4$

c. $7^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(7) = 4$

d. $9^2 \equiv 1 \bmod (10) \rightarrow \text{ord}(9) = 2$

Primitive Roots

- Primitive Roots In the group G = $<Z_n*, \times>$, when the order of an element is the same as $\phi(n)$, that element is called the primitive root of the group.

- If p is a prime, a primitive root mod p is a number g whose power yield every nonzero class mod p. $\{gk|0<k<p\}=\{1,2,\ldots,p-1\}$

Proposition: Let g be a primitive root mod p

$g^n \equiv 1 \pmod{p}$ if $n \equiv 0 \pmod{p-1}$

$g^j \equiv g^k \pmod{p}$ if $j \equiv k \pmod{p-1}$

Example 3 is a primitive root mod 7 but not for mod 13

Mathematics of Cryptography