Divisibility

- We say that a nonzero b **divides** a if $a = mb$ for some m, where a, b, and m are integers
- b divides a if there is no remainder on division
- The notation $b \mid a$ is commonly used to mean b divides a
- If $b \mid a$ we say that b is a **divisor** of a

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24
$13 \mid 182$; $-5 \mid 30$; $17 \mid 289$; $-3 \mid 33$; $17 \mid 0$

Properties of Divisibility

- If $a \mid 1$, then $a = \pm 1$
- If $a \mid b$ and $b \mid a$, then $a = \pm b$
- Any $b \neq 0$ divides 0
- If $a \mid b$ and $b \mid c$, then $a \mid c$

$$\boxed{11 \mid 66 \text{ and } 66 \mid 198 = 11 \mid 198}$$

- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n

Properties of Divisibility

- To see this last point, note that:
  - If $b \mid g$, then g is of the form $g = b * g_1$ for some integer g_1
  - If $b \mid h$, then h is of the form $h = b * h_1$ for some integer h_1
- So:
  - $mg + nh = mbg_1 + nbh_1 = b * (mg_1 + nh_1)$

    and therefore b divides $mg + nh$

> $b = 7$; $g = 14$; $h = 63$; $m = 3$; $n = 2$
> $7 \mid 14$ and $7 \mid 63$.
> To show 7 (3 * 14 + 2 * 63),
> we have (3 * 14 + 2 * 63) = 7(3 * 2 + 2 * 9),
> and it is obvious that $7 \mid (7(3 * 2 + 2 * 9))$.

Contd...

- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n.

To see this last point, note that

- If $b|g$, then g is of the form $g = b \times g_1$ for some integer g_1.
- If $b|h$, then h is of the form $h = b \times h_1$ for some integer h_1.

So

$$mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1)$$

and therefore b divides $mg + nh$.

$b = 7; g = 14; h = 63; m = 3; n = 2$
$7|14$ and $7|63$.
To show $7|(3 \times 14 + 2 \times 63)$,
we have $(3 \times 14 + 2 \times 63) = 7(3 \times 2 + 2 \times 9)$,
and it is obvious that $7|(7(3 \times 2 + 2 \times 9))$.

Division Algorithm

- Given any positive integer n and any nonnegative integer a, if we divide a by n we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \qquad 0 \leq r < n; \; q = [a/n]$$

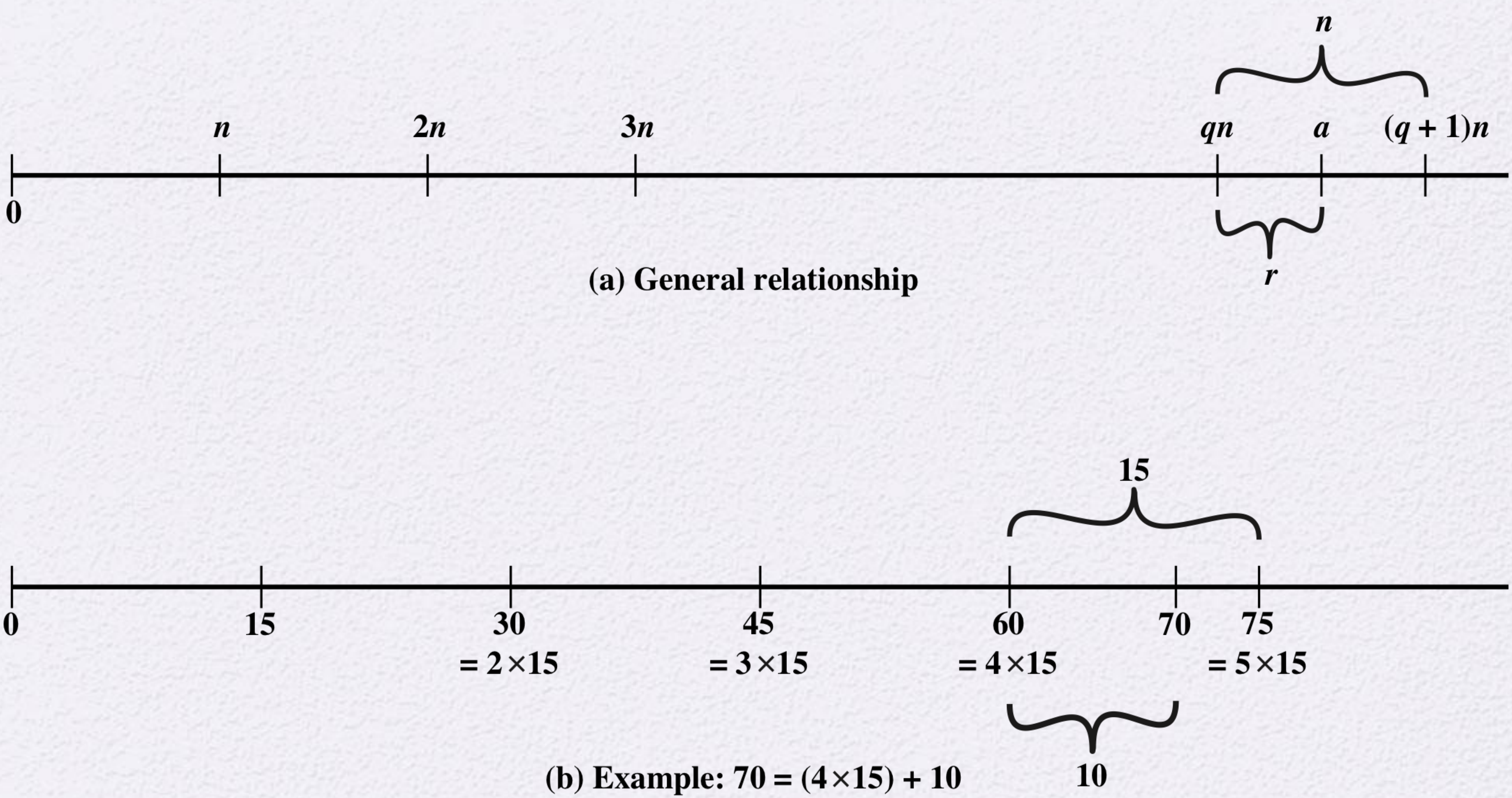

Figure 4.1 The Relationship $a = qn + r;\ 0 \leq r < n$

Euclidean Algorithm

- One of the basic techniques of number theory
- Procedure for determining the greatest common divisor of two positive integers
- Two integers are **relatively prime** if their only common positive integer factor is 1

Greatest Common Divisor (GCD)

- The greatest common divisor of *a* and *b* is the largest integer that divides both *a* and *b*

- We can use the notation gcd(*a*,*b*) to mean the **greatest common divisor** of *a* and *b*

- We also define gcd(0,0) = 0

- Positive integer *c* is said to be the gcd of *a* and *b* if:
  - *c* is a divisor of *a* and *b*
  - Any divisor of *a* and *b* is a divisor of *c*

- An equivalent definition is:

$$\gcd(a,b) = \max[k, \text{ such that } k \mid a \text{ and } k \mid b]$$

GCD

- Because we require that the greatest common divisor be positive, gcd(a,b) = gcd(a,$-b$) = gcd($-a$,b) = gcd($-a$,$-b$)
- In general, gcd(a,b) = gcd($|a|$, $|b|$)

gcd(60, 24) = gcd(60, - 24) = 12

- Also, because all nonzero integers divide 0, we have gcd(a,0) = $|a|$
- We stated that two integers *a* and *b* are relatively prime if their only common positive integer factor is 1; this is equivalent to saying that *a* and *b* are **relatively prime** if gcd(a,b) = 1

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

Algorithm

```
GCD(a,b):
    A=a, B=b
     while B>0
         R = A mod B
         A = B, B = R
     return A
```

GCD(1970,1066)

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

Table 4.1
Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q_1 = 3	r_1 = 211943424
b = 316258250	r_1 = 211943424	q_2 = 1	r_2 = 104314826
r_1 = 211943424	r_2 = 104314826	q_3 = 2	r_3 = 3313772
r_2 = 104314826	r_3 = 3313772	q_4 = 31	r_4 = 1587894
r_3 = 3313772	r_4 = 1587894	q_5 = 2	r_5 = 137984
r_4 = 1587894	r_5 = 137984	q_6 = 11	r_6 = 70070
r_5 = 137984	r_6 = 70070	q_7 = 1	r_7 = 67914
r_6 = 70070	r_7 = 67914	q_8 = 1	r_8 = 2156
r_7 = 67914	r_8 = 2156	q_9 = 31	r_9 = 1078
r_8 = 2156	r_9 = 1078	q_{10} = 2	r_{10} = 0

(This table can be found on page 91 in the textbook)

Modular Arithmetic

- The modulus
  - If *a* is an integer and *n* is a positive integer, we define *a* mod *n* to be the remainder when *a* is divided by *n;* the integer *n* is called the **modulus**
  - thus, for any integer *a:*

    $a = qn + r \quad 0 \le r < n; \; q = [a/n]$

    $a = [a/n] * n + (a \bmod n)$

Negative number modulo k = k minus positive number modulo k. To find (–n)%k = k–(n%k)

11 mod 7 = 4; - 11 mod 7 = 3

Modular Arithmetic

- Congruent modulo n
  - Two integers a and b are said to be **congruent modulo n** if $(a \bmod n) = (b \bmod n)$
  - This is written as $a = b(\text{mod } n)$[2]
  - Note that if $a = 0(\text{mod } n)$, then $n \mid a$

$73 = 4 \ (\text{mod } 23)$; $21 = -9 \ (\text{mod } 10)$

Properties of Congruences

- Congruences have the following properties:

  1. $a = b \pmod{n}$ if $n\ (a - b)$

  2. $a = b \pmod{n}$ implies $b = a \pmod{n}$

  3. $a = b \pmod{n}$ and $b = c \pmod{n}$ imply $a = c \pmod{n}$

- To demonstrate the first point, if $n\ (a - b)$, then $(a - b) = kn$ for some k
  - So we can write $a = b + kn$
  - Therefore, (a mod n) = (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) = (b mod n)

23 = 8 (mod 5) because 23 - 8 = 15 = 5 * 3
- 11 = 5 (mod 8) because - 11 - 5 = - 16 = 8 * (- 2)
81 = 0 (mod 27) because 81 - 0 = 81 = 27 * 3

Modular Arithmetic

- Modular arithmetic exhibits the following properties:

    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. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

- We demonstrate the first property:
    - Define $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$. Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer k
    - Then:

$$\begin{aligned}(a + b) \bmod n &= (ra + jn + rb + kn) \bmod n \\ &= (ra + rb + (k + j)n) \bmod n \\ &= (ra + rb) \bmod n \\ &= [(a \bmod n) + (b \bmod n)] \bmod n\end{aligned}$$

Remaining Properties:

- Examples of the three remaining properties:

11 mod 8 = 3; 15 mod 8 = 7

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2

(11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) - (15 mod 8)] mod 8 = - 4 mod 8 = 4

(11 - 15) mod 8 = - 4 mod 8 = 4

[(11 mod 8) * (15 mod 8)] mod 8 = 21 mod 8 = 5

(11 * 15) mod 8 = 165 mod 8 = 5

To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 \equiv 4 \pmod{13}$$

$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$

$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

Table 4.2(a) Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Table 4.2(b) Multiplication Modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Table 4.2(c)

Additive and Multiplicative Inverses Modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Contd…

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n - 1)\}$$

This is referred to as the **set of residues**, or **residue classes** (mod n). To be more precise, each integer in Z_n represents a residue class. We can label the residue classes (mod n) as $[0], [1], [2], \ldots, [n - 1]$, where

$$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$$

The residue classes (mod 4) are

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

Table 4.3

Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse ($-w$)	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

if $(a + b) \equiv (a + c) \pmod{n}$ **then** $b \equiv c \pmod{n}$ **(4.4)**

$$\boxed{(5 + 23) \equiv (5 + 7)(\text{mod}\,8);\ 23 \equiv 7(\text{mod}\,8)}$$

if $(a \times b) \equiv (a \times c)(\text{mod}\ n)$ **then** $b \equiv c\ (\text{mod}\ n)$ **if** a is relatively prime to n **(4.5)**

Recall that two integers are **relatively prime** if their only common positive integer factor is 1. Similar to the case of Equation (4.4), we can say that Equation (4.5) is

$$((a^{-1})ab) \equiv ((a^{-1})ac)(\text{mod}\,n)$$

$$b \equiv c(\text{mod}\,n)$$

To see this, consider an example in which the condition of Equation (4.5) does not hold. The integers 6 and 8 are not relatively prime, since they have the common factor 2. We have the following:

$$6 \times 3 = 18 \equiv 2 \pmod 8$$
$$6 \times 7 = 42 \equiv 2 \pmod 8$$

Yet $3 \not\equiv 7 \pmod 8$.

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

$$\boxed{\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11) = 11}$$

Extended Euclidean

- The extended Euclidean algorithm not only calculate the greatest common divisor *d but also two additional integers x* and *y that satisfy the following equation.*

- *It is whole numbers – cannot tolerate fractions*

$$ax + by = d = \gcd(a, b)$$

Extended Euclidean

Example 1: $m = 65, n = 40$

Step 1: The (usual) Euclidean algorithm:

$$\begin{array}{lrcl}
(1) & 65 & = & 1 \cdot 40 + \boxed{25} \\
(2) & 40 & = & 1 \cdot \boxed{25} + 15 \\
(3) & \boxed{25} & = & 1 \cdot 15 + 10 \\
(4) & 15 & = & 1 \cdot 10 + 5 \\
 & 10 & = & 2 \cdot 5
\end{array}$$

Therefore: $\gcd(65, 40) = 5$.

Step 2: Using the method of back-substitution:

$$\begin{aligned} 5 &\overset{(4)}{=} 15 - 10 \\ &\overset{(3)}{=} 15 - (25 - 15) &&= 2 \cdot 15 - 25 \\ &\overset{(2)}{=} 2(40 - 25) - 25 &&= 2 \cdot 40 - 3 \cdot 25 \\ &\overset{(1)}{=} 2 \cdot 40 - 3(65 - 40) &&= 5 \cdot 40 - 3 \cdot 65 \end{aligned}$$

Conclusion: $65(-3) + 40(5) = 5$.

Example 2: $m = 1239, n = 735$

Step 1: The (usual) Euclidean algorithm:

$$\begin{array}{lllll}
(1) & 1239 & = 1 \cdot 735 & + & \boxed{504} \\
(2) & 735 & = 1 \cdot \boxed{504} & + & 231 \\
(3) & \boxed{504} & = 2 \cdot 231 & + & 42 \\
(4) & 231 & = 5 \cdot 42 & + & 21 \\
 & 42 & = 2 \cdot 21 & &
\end{array}$$

Therefore: $\gcd(1239, 735) = 21$.

Step 2: Using the method of back-substitution:

$$
\begin{aligned}
21 &\overset{(4)}{=} 231 \; - \; 5 \cdot 42 \\
&\overset{(3)}{=} 231 - 5(504 - 2 \cdot 231) &&= 11 \cdot 231 - 5 \cdot 504 \\
&\overset{(2)}{=} 11(735 - 504) - 5 \cdot 504 &&= 11 \cdot 735 - 16 \cdot 504 \\
&\overset{(1)}{=} 11 \cdot 735 - 16(1239 - 735) &&= 27 \cdot 735 - 16 \cdot 1239
\end{aligned}
$$

Conclusion: $1239(-16) + 735(27) = 21$.

Contd…

- Find the inverse of 15 mod 26.
- GCD(26,15) = GCD(15,11) = GCD(11,4) = GCD(4,3) =GCD(3,1)= GCD(1,0) =1 Co-prime.
- Extended Euclidean algorithm.
- 26 = 1*26 + 0*15
- 15 = 0*26 + 1*15

Contd…

- 11 = Equ 1 – Equ 2 = 1 * 26 – 1*15
- 4 = Equ 2 – Equ 3 = -1 * 26 + 2* 15
- 3 = Equ3 – 2 * Equ 4 = 3*26 -5*15
- 1 = Equ 4 – Equ 5 = -4 *26 + 7 *15.
- Co-efficient is inverse. i.e., 7.

Contd…

- Find inverse of 21 mod 26.
- GCD(26,21) =1.
- 5

CRT

- The Chinese remainder theorem is a theorem of number theory, which states that, if one knows the remainders of the division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime.

Contd…

- $Z = C_i \bmod b_i = 3 \bmod 8, 1 \bmod 9, 4 \bmod 11$
- Then $Z = B_1X_1C_1 + B_2X_2C_2 + B_3X_3C_3$

  $= B_1X_1*3 + B_2X_2*1 + B_3X_3*4$

  B = product of divisors = $8*9*11 = 792$

  $B_1 = B/b_i = 792/8 = 99$

  $B_2 = 88$, $B_3 = 72$

  $B_1X_1 \equiv 1 \bmod b_1$.

  $Z = 99.3.3 + 88(-5).1 + 72.2.4 = 1027$

  - Carmichael numbers 561

GCD(42,30) =6

x / y	−3	−2	−1	0	1	2	3
−3	−216	−174	−132	−90	−48	−6	36
−2	−186	−144	−102	−60	−18	24	66
−1	−156	−114	−72	−30	12	54	96
0	−126	−84	−42	0	42	84	126
1	−96	−54	−12	30	72	114	156
2	−66	−24	18	60	102	144	186
3	−36	6	48	90	132	174	216

Table 4.4
Extended Euclidean Algorithm Example

i	r_i	q_i	x_i	Y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: d = 1; x = –111; y = 355

Groups

- A set of elements with a binary operation denoted by • that associates to each ordered pair (a,b) of elements in G an element (a • b) in G , such that the following axioms are obeyed:
  - (A1) Closure:
    - If a and b belong to G, then a • b is also in G
  - (A2) Associative:
    - a • (b • c) = (a • b) • c for all a, b, c in G
  - (A3) Identity element:
    - There is an element e in G such that a • e = e • a = a for all a in G
  - (A4) Inverse element:
    - For each a in G, there is an element a in G such that a•a = a • a = e
  - (A5) Commutative:
    - a • b = b • a for all a, b in G

- Obeys CAIN:
  - Closure : a,b in S, then a.b in S
  - Associative law :(a.b).c = a.(b.c)
  - has Identity e :e.a = a.e = a
  - has Inverses a-1 :$a.a^{-1} = e$

- if commutative a.b = b.a
  - then forms an abelian group

If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group. Otherwise, the group is an **infinite group**.

A group is said to be **abelian** if it satisfies the following additional condition:

(A5) Commutative: $a \cdot b = b \cdot a$ for all a, b in G.

Example

- The set of integers (positive, negative, and 0) under addition is an abelian group.
- The set of nonzero real numbers under multiplication is an abelian group.

Cyclic Group

- Exponentiation is defined within a group as a repeated application of the group operator, so that $a^3 = a \bullet a \bullet a$
- We define $a^0 = e$ as the identity element, and $a^{-n} = (a')^n$, where a' is the inverse element of a within the group
- A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element
- The element a is said to **generate** the group G or to be a **generator** of G
- A cyclic group is always abelian and may be finite or infinite

Example

$\mathbb{Z}_N$ = {0, …, N-1} under addition modulo N

– Identity is 0
– Inverse of a is [-a mod N]
– Associativity, commutativity obvious
– Order N

– $m \cdot a = a + \cdots + a \bmod N$
  - Can be computed efficiently

Contd…

- Modular Inverses uses gcd, inverse of b mod N
- Gcd(b,N) =1.

Contd…

- If p is prime, then 1, 2, 3, …, p-1 are all invertible modulo p

- If N=pq for p, q distinct primes, then the invertible elements are the integers from 1 to N-1 that are *not* multiples of p or q

$\mathbb{Z}^*_N$ = invertible elements between 1 and N-1 under multiplication modulo N

- Closure not obvious, but can be shown
- Identity is 1
- Inverse of a is $[a^{-1} \bmod N]$
- Associativity, commutativity obvious

- $a^m = a \cdots a \bmod N$

Contd…

$\phi(N)$ = the number of invertible elements modulo N

$= |\{a \in \{1, \ldots, N-1\} : \gcd(a, N) = 1\}|$

= The order of $\mathbb{Z}^*_N$

– If N is prime, then $\phi(N) = N-1$

– If N=pq, p and q distinct primes, $\phi(N)$ = ?

$\phi(21) = \phi(3) \times \phi(7) = (3-1) \times (7-1) = 2 \times 6 = 12$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8