Integer Arithmetic

Gunjan.Rehani@bennett.edu.in, Madhushi.Verma@bennett.edu.in

CSE, SEAS
Bennett University

June 14, 2021

Overview

Introduction

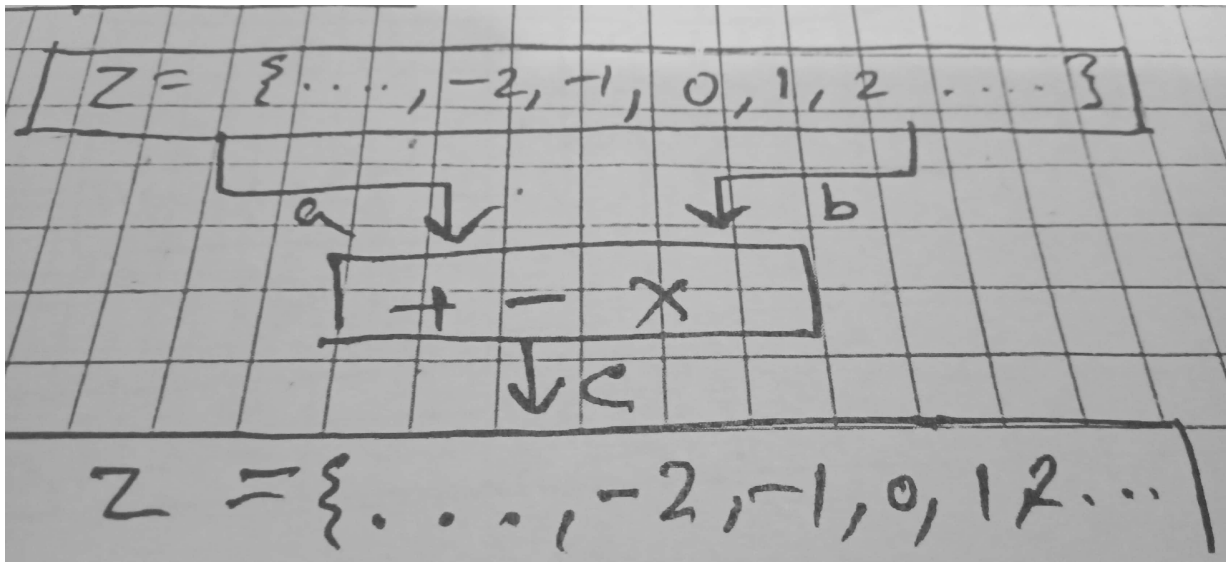
Set of Integers : Denoted by Z, contains all integral numbers (with no fraction), from negative infinity to positive infinity.
$Z = \{... -2, -1, 0, 1, 2...\}$
Real life examples:

- Number of books in a bookshelf
- Number of students in a class
- Temperature value(40 degrees, -20 degrees)

The branch of mathematics that involves integers, and the properties of integer is called Number Theory.
It has important applications in Cryptography and Network Security.

Binary Operations

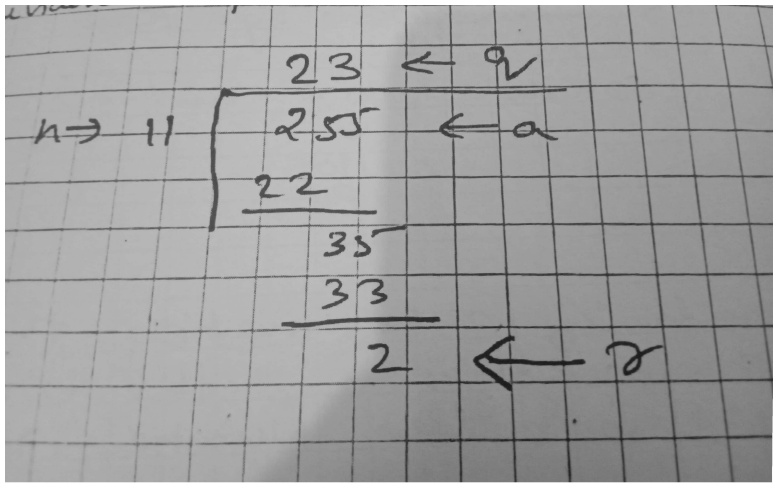
$+, -, \times$ operations



eg. $5 + 9 = 14$
$5 - 9 = -4$
$5 \times 9 = 45$

Integer Division

In Integer arithmetic, if we divide a by n, we get q and r.
The relationship can be shown as:-
$a = q \times n + r$
where a= dividend. q=quotient,n=divisor and r=remainder



The divisor should be a positive integer($n > 0$).
The remainder should be a non-negative integer($r >= 0$).

Divisibility

If $a \neq 0$ and we let r=0, in the division relation,we get
$a = q \times n$ i.e a is divisible by n, also written as $n|a$
eg. The integer 4 divides the integer 32, because $32 = 8 \times 4$. Therefore, it can be written as $4|32$

Properties of Divisibility:

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.

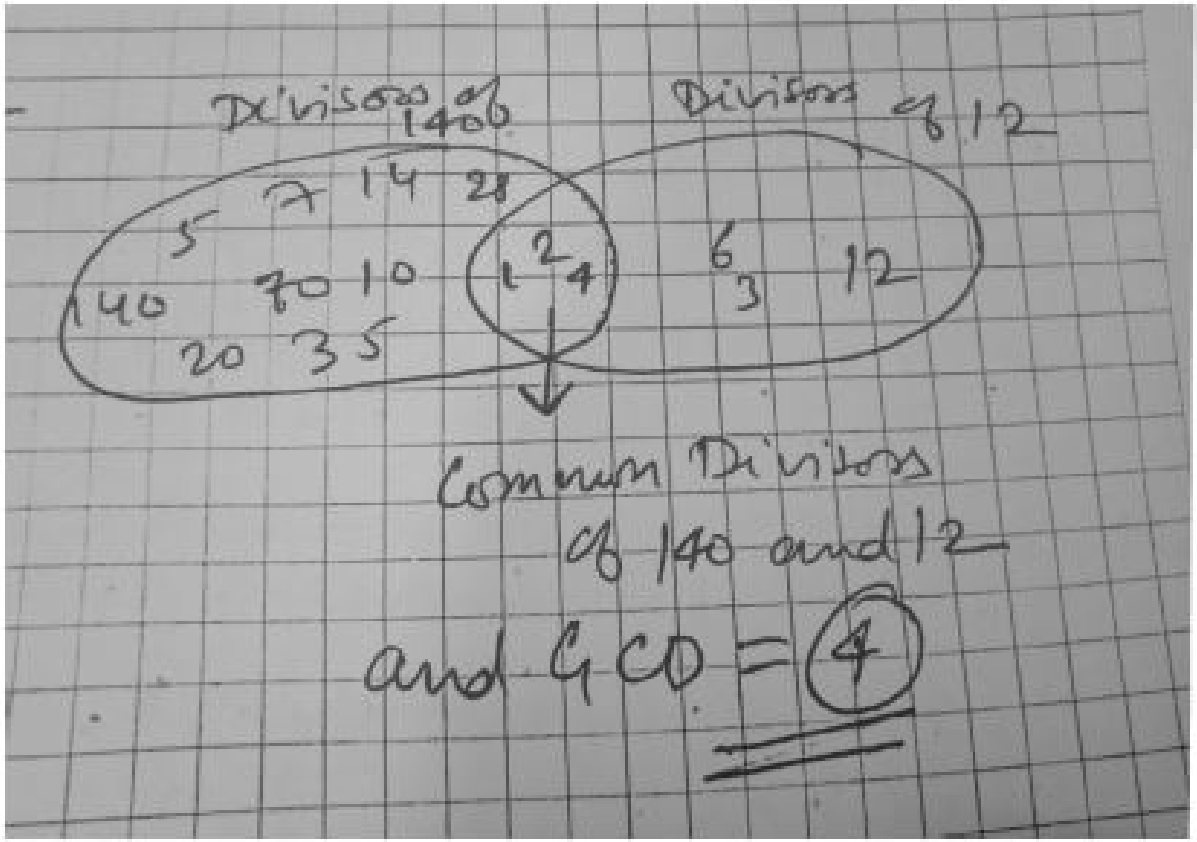
Greatest Common Divisor (GCD)

eg. Let us assume we have 24 black pens and 30 blue pens.
We want to distribute the pens among a group of students, such that each student gets an equal number of black and blue pens.
The size of the largest such group can be determined by finding the GCD of 24 and 30.

Solution

A group of 6 students. Each gets 4 black and 5 blue pens.(6 is the GCD of 24 and 30)

Example 2


Divisors of 140
5 7 14 28
140 70 10 20 35
Divisors of 12
1 2 4
6 3 12
Common Divisors
of 140 and 12
and GCD = 4

Euclidean Theorem to find GCD

Euclidean-Algorithm (a,b)

Step 1 : $r \leftarrow a$, $s \leftarrow b$

Step 2 : while $s \neq 0$, repeat Step 3 and 4

Step 3 : $t = rmods$

Step 4 : $r \leftarrow s$, $s \leftarrow t$

Step 5 : $d \leftarrow r$

Fact 1 : gcd(a,0)=a

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

eg. if we find gcd of (25,60) using Euclidean Algorithm

q	r	s	t
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

Answer is 5

Try Yourself

1. gcd(2740,1760)
2. gcd(875,288)