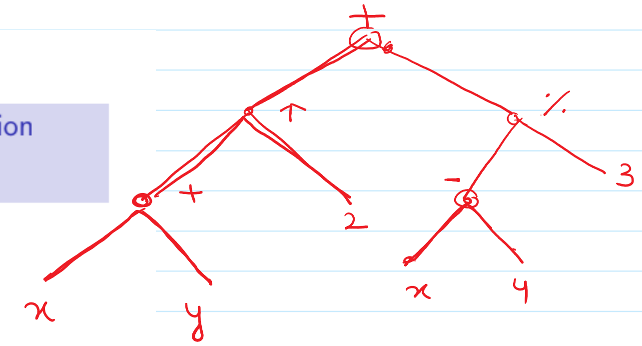
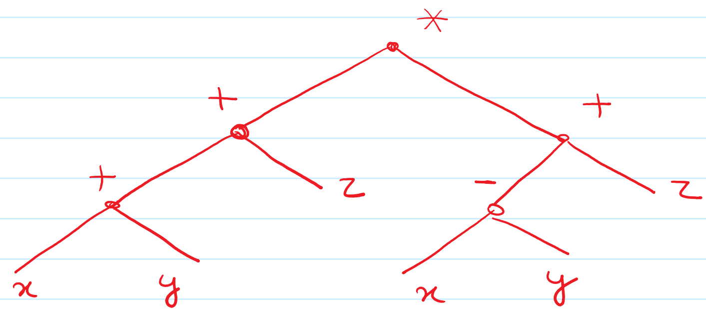
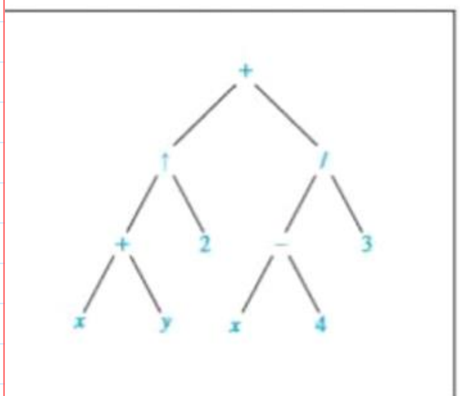
What is the ordered rooted tree that represents the expression $((x+y)\uparrow 2)+((x-4)/3)$?



$((x+y)+z) * ((x-y)+z)$





$((x+y)\uparrow 2)+((x-4)/3)$.

infix notation.

A + B (infix notation)

+ A B (Prefix notation)

A B + (Post fix notation)

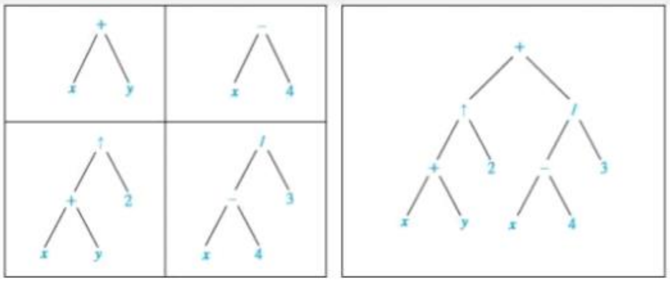
What is the prefix form for $((x+y)\uparrow 2)+((x-4)/3)$?

We obtain the prefix form of an expression when we traverse its rooted tree in preorder. Expressions written in prefix form are said to be in **Polish notation**, which is named after the Polish logician Jan Lukasiewicz.

$((+xy)\uparrow 2)+((-x4)/3)$

$(\uparrow +xy2) + (/-x43)$

$+\uparrow+xy2/-x43$ Ans.



A binary tree representing $((x + y) \uparrow 2) + ((x - 4)/3)$.

Solution: We obtain the prefix form for this expression by traversing the binary tree that represents it in preorder This produces $+ \uparrow + x\ y\ 2\ / - x\ 4\ 3$.

What is the postfix form of the expression
$((x + y) \uparrow 2) + ((x - 4)/3)$?

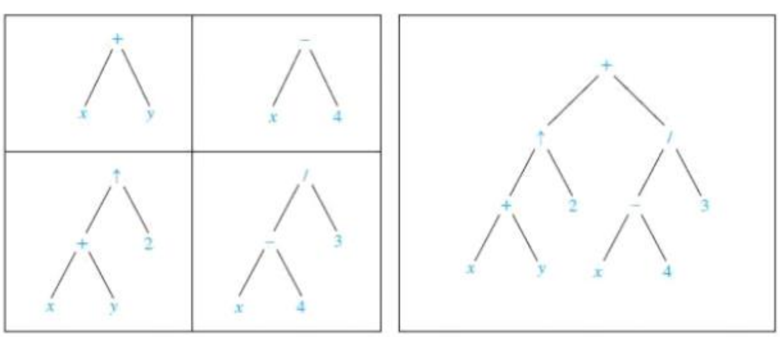
$((xy+) \uparrow 2) + ((x4-)/3)$

$(xy+2\uparrow) + (x4-3/)$

$xy+2\uparrow\ x4-3/+$

$x+y \rightarrow (xy+)$

What is the postfix form of the expression $((x + y) \uparrow 2) + ((x - 4)/3)$?



Solution: The postfix form of the expression is obtained by carrying out a postorder traversal of the binary tree for this expression This produces the postfix expression: $x\ y + 2 \uparrow x\ 4 - 3 / +$.

What is the value of the prefix expression $+ - * 2\ 3\ 5 / \uparrow 2\ 3\ 4$?

Right of left

$+ \quad - \quad * \quad 2 \quad 3 \quad 5 \quad / \quad \uparrow \quad 2 \quad 3 \quad 4$

$2 \uparrow 3 = 8$

$+ \quad - \quad * \quad 2 \quad 3 \quad 5 \quad / \quad 8 \quad 4$

$8/4 = 2$

$+ \quad - \quad * \quad 2 \quad 3 \quad 5 \quad 2$

$2 * 3 = 6$

$+ \quad - \quad 6 \quad 5 \quad 2$

$6 - 5 = 1$

$+ \quad 1 \quad 2$

$1 + 2 = 3$

Value of expression: 3

Evaluating a prefix expression.

$/84 \rightarrow 8/4 \quad 2 \uparrow 3$

$+ - * 2\ 3\ 5 / \uparrow 2\ 3\ 4$

$+ - * 2\ 3\ 5 / 8\ 4$

$+ - * 2\ 3\ 5\ 2$

$2 * 3$

$+ - 6\ 5\ 2$

$+ 1\ 2$

3

What is the value of the postfix expression $7\ 2\ 3 * - 4 \uparrow 9\ 3 / +$?

23 ×

$2 * 3 = 6$

$7 \quad 2 \quad 3 \quad * \quad - \quad 4 \quad \uparrow \quad 9 \quad 3 \quad / \quad +$

$2 * 3 = 6$

$7 \quad 6 \quad - \quad 4 \quad \uparrow \quad 9 \quad 3 \quad / \quad +$

$7 - 6 = 1$

$1 \quad 4 \quad \uparrow \quad 9 \quad 3 \quad / \quad +$

$1^4 = 1$

$1 \quad 9 \quad 3 \quad / \quad +$

$9/3 = 3$

$1 \quad 3 \quad +$

$1 + 3 = 4$

Value of expression: 4

Evaluating a postfix

$7\ 6 - 4 \uparrow 9\ 3 / +$

$1\ 4 \uparrow 9\ 3 / +$

$1\ 9\ 3 / +$

$1\ 3 +$

$1 + 3 = 4$

4

UNIT 6 : Number Theory and Cryptography

- Number Theory
- Division
- Division Algorithm
- Modular Arithmetic
- Arithmetic Modulo m
- Quiz

Division

When one integer is divided by a second non-zero integer, the quotient may or may not be an integer. For example, $12/4=3$, an integer but $11/4=2.75$, not an integer.

Example 1

Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Properties of divisibility of integers

Let a, b and c are integers, where $a \neq 0$. Then,

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

(ii) if $a \mid b$, then $a \mid bc$ for all integers c;

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

What are the quotient and remainder when 101 is divided by 11?

What are the quotient and remainder when -11 is divided by 3?

A. -4,1

B. -3,1

C. 2,-3

D. -3,-1

What are the quotient and remainder when -11 is divided by 3?

A. -4,1

B. -3,1

C. 2,-3

D. -3,-1

Answer : A.

Theorem 1 : Let a and b be integers, and let m be a positive integer Then, $a \equiv b(\text{mod } m)$ if and only if $a\text{mod } m = b(\text{mod } m)$.

Example: Determine whether 17 is congruent to 5 modulo 6?
Solution : We have $17 - 5 = 12$ and 6 divided 12 as $12/6 = 2$, an integer, so 17 is congruent to 5 modulo 6. That is,

$$17 \equiv 5(\text{mod } 6).$$

Modular Arithmetic

Theorem 2 : Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Theorem 3 : Let m be a positive integer. If $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then

$$a + c \equiv b + d(\text{mod } m), \qquad ac \equiv bd(\text{mod } m).$$

Since $7 \equiv 2 (\text{mod } 5)$ and $11 \equiv 1 (\text{mod } 5)$, so

$$18 = 7 + 11 \equiv 2 + 1 \equiv 3 (\text{mod } 5)$$

and

$$77 = 7.11 \equiv 2.1 \equiv 2 (\text{mod } 5).$$

Use the definition of addition and multiplication in $\mathbb{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Which is equivalent to 3 modulo 7?

A. 37
B. 66
C. -17
D. -69

Answer : B

The inverse of 6 in $\mathbb{Z}_{13}$ is

A. 5

B. 6

C. 7

D. -3