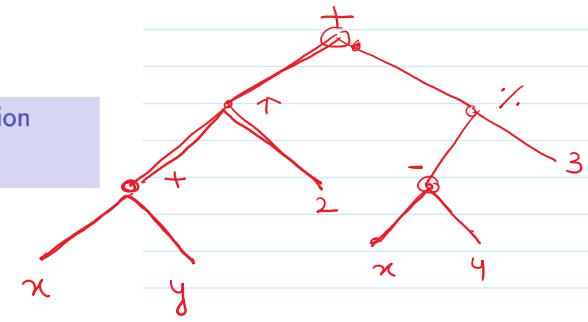
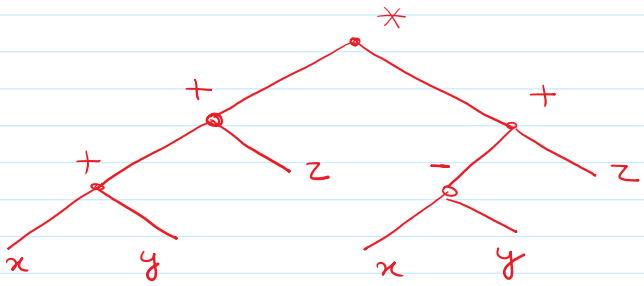
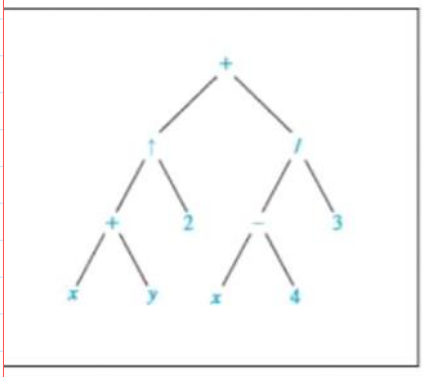
What is the ordered rooted tree that represents the expression $((x+y)\uparrow 2)+((x-4)/3)$?



$((x+y)+z) \neq ((x-y)+z)$





((x + y) ↑ 2) + ((x − 4)/3).

Infix notation.

A + B (infix notation)

+ A B (Prefix notation)

A B + (Post fix notation)

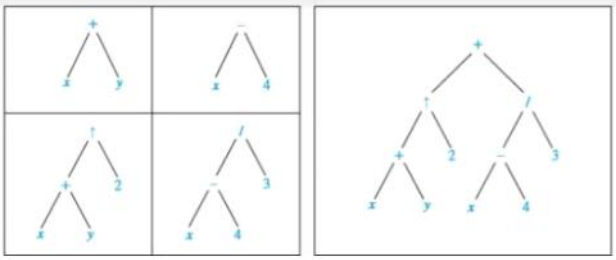
What is the prefix form for $((x+y)\uparrow 2)+((x-4)/3)$?

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

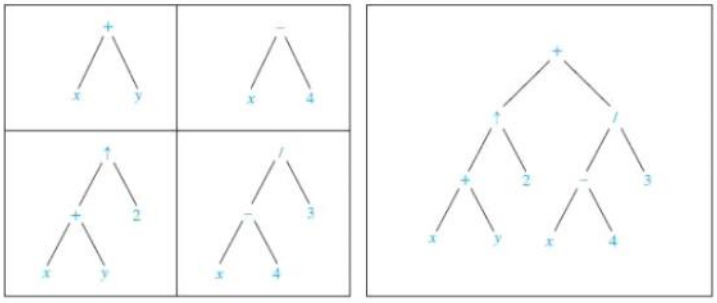
$((xy+)\uparrow 2) + ((x4-)/3)$

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

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

$x+y \rightarrow (xy+)$

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 / ↑ 2 3 4?

Right of left

/84 → 8/4 2↑3

+ − ∗ 2 3 5 / ↑ 2 3 4

2↑3 = 8

+ − ∗ 2 3 5 / 8 4

8/4 = 2

+ − ∗ 2 3 5 2

2∗3 = 6

+ − 6 5 2

6−5 = 1

+ 1 2

1+2 = 3

Value of expression: 3 ✓

+ − ∗ 2 3 5 / ↑ 2 3 4 ←

+ − ∗ 2 3 5 / 8 4

+ − ∗ 2 3 5 2 ← 2∗3

+ − 6 5 2

+ 1 2

3 ✓

Evaluating a prefix expression.

What is the value of the postfix expression 7 2 3 ∗ −4 ↑ 9 3/+?

23 X

2∗3 = 6

7 2 3 ∗ − 4 ↑ 9 3 / +

2∗3 = 6

7 6 − 4 ↑ 9 3 / +

7−6 = 1

1 4 ↑ 9 3 / +

$1^4 = 1$

1 9 3 / +

9/3 = 3

1 3 +

1+3 = 4

Value of expression: 4

76 − 4 ↑ 93/+

14 ↑ 93/+

193/+

13+ 1+3=4

4

Evaluating a postfix

UNIT 6 : Number Theory and Cryptography

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

Division

Open with Google Docs

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.

e.g. $\frac{12}{4} = 3 \Rightarrow 12 = 4 \cdot 3$

$\frac{11}{4} = 2.75 \Rightarrow 4 \nmid 11$

$4 \nmid 11$

Let $a \in \mathbb{Z}$ be any integer and b is a +ve integer then we say that b divides a if $\exists$ an integer c s.t

$\frac{a}{b} = c$

or $a = bc$.

$b \mid a = \frac{a}{b}$

$a = bc$

$b \mid a = \frac{a}{b}$

Example 1

$\frac{7}{3} = 2.333$

$3 \nmid 7$

$\frac{12}{3} = 4$

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

(i) $3 \nmid 7$

(ii) $3 \mid 12$ yes $\frac{12}{3} = 4$

Properties of divisibility of integers

$3|6,\ 3|9 \Rightarrow 3|(6+9)$

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

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

$2|4,\ 2|6$ then $2|(4+6)$

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

$2|4,\ 2|4.6$

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

Transitivity of number

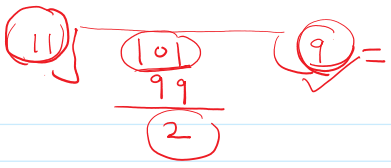
$2|4,\ 4|8$ then $2|8$

$a|b$ then $a|bc$

$2|6$ $\quad 2|6.3$

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

$101 = 11(9) + 2$ (9 = q, 2 = R.)



Quotient = 9

Remainder = 2

Dividend = Divisor × Quotient + Remainder

$a = bq + r$ $\quad 0 \le r < b$

(N1) remainder is always positive or zero.

Q Which are quotient and remainder when -11 is divided by 3.

$q =$ ___ $\quad r =$ ___

$-11 = 3(-3) - 2$ (q, r)

$r = -2$ ✗

$-11 = 3(-4) + 1$ ✓

Quotient $= -4$ ✓

Remainder $= 1$ ✓

$26 = 5(-6) + 4$

Quotient $= -6$

Remainder $= 4$.

if -26 is divided by 5 what are quotient and remainder.

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

A. -4,1

B. -3,1

C. 2,-3

D. -3,-1

Q When -21 is divided by 5. then what are quotient and remainder

(a) $-3, 5$

(b) $-4, 2$

$-21 = 5(-5) + 4$

Quotient $= -5$

(b) -4, 2

(c) -5, 4

(d) -5, 3.

$-11 = 3(-5) + 4$

Quotient $= -5$

Remainder $= 4$.

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, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \pmod{m}$.

$a \equiv b \pmod{m}$ if $m \mid (a-b)$

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,

$$17 \equiv 5 \pmod{6}.$$

$17 \equiv 5 \pmod{6}$

$6 \mid 17-5$

$6 \mid 12$

$17 \equiv 5 \pmod 6$.

$6 \mid 17-5$

$6 \mid 12$

$13 \equiv 8 \pmod 4$

$4 \mid 13-8$

4×5

$26 \equiv 1 \pmod 5$

(a) 2 (b) 3 (c) 4 (d) 1

Modular Arithmetic

$a \equiv b \pmod m$

$a = mk + b$

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 $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

$$a + c \equiv b + d \pmod m, \qquad ac \equiv bd \pmod m.$$

$a \equiv b \pmod m$

$m \mid (a-b)$

$\therefore \exists$ an integer k s.t

$\frac{a-b}{m} = k$

$a - b = mk$

$a = mk + b$

$11 \equiv 2 \pmod 3$, $10 \equiv 1 \pmod 3$

$21 \equiv 3 \pmod 3$ $110 \equiv 2 \pmod 3$

$21 = 0 \pmod 3$

$26 \equiv 2 \pmod 3$

$25 = 1 \pmod 3$

$26 \times 25 = 2 \pmod 3$

Addition in modular Arithmetic.

$Z_m = \{0, 1, 2, 3, \ldots, m-1\}$

$Z_5 = \{0, 1, 2, 3, 4\}$

$3 +_5 4 = 7 \pmod 5 = 2$

$1 +_5 3 = 4$

$3 \times_5 4 = 12 \pmod 5$

$= 2 \pmod 5$

$2 \times_5 4 = 8 \pmod 5$

$= 3 \pmod 5$

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

$\mathbb{Z}_{11} = \{0, 1, 2, \ldots, 10\}$

$7 +_{11} 9 = 16 \pmod{11} = 5$

$7 \times_{11} 9 = 63 \pmod{11} = 8$.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5, 6\}$

Which is equivalent to 3 modulo 7?

A. 37 ✗

B. 66 ✓

C. -17 ✗

D. -69 ✗

Answer : B

$-17 + 21 = 4$

$-17 + 7 = -10$

$-17 + 14 = -3$

$-17 + 21 = 4$

$4 \equiv 4 \pmod 7$

$7 \mid 4 - 4$

$7 \mid 0$

$-69 + 70 = 1$

$1 \equiv 1 \pmod 7$

Q Find the inverse of 7 (mod 5)

$7 \times 3 = 21 \pmod 5$

$= 1 \pmod 5$

$a\,b = 1$

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

A. 5 ✗

B. 6 ✗

C. 7 ✗

D. -3 ✗

inverse of 7 is 3 ✗

$-3 + 13 = 10$

$6 \times 5 = 30 \pmod{13} = 4 \pmod{13}$

$6 \times 6 = 36 \pmod{13} = 10 \pmod{13}$

$7 \times 6 = 42 \pmod{13} = 3 \pmod{13}$

$6 \cdot 10 = 60 \pmod{13}$

$= 8 \pmod{13}$

$7 \times 1 = 7 \pmod 5$

EXERCISE 1.1

1. Use Euclid's division algorithm to find the HCF of :

(i) 135 and 225 (ii) 196 and 38220 (iii) 867 and 255

135 | 225 | 1
135
90 | 135 | 1
90
45 | 90 | 2
90
→ X

H.C.F = (135, 225) = 45

225 = 135.1 + 90
135 = 90.1 + 45
90 = 45.2 + 0 ×

45 = 135 − 90.1
= 135 − {225 − 135.1} ×1
= 1.135 − 225.1 + 135.1
= 2.135 + 225(−1)

45 = x(135) + y(225)

$x = 2$, $y = -1$ are called Bezout's coefficient

45 = x (135) + y (225)

(a) $x = 2$, $y = 2$ ×
(b) $x = -2$, $y = -2$ ×
(c) $x = 2$, $y = -1$ ✓
(d) $x = 3$, $y = 3$ ×

$255 \overline{)\ 867\ (3}$
765

$102 \overline{)\ 255\ (2}$
204

$51 \overline{)\ 102\ (2}$
102
$\times$

H.C.F $(255, 867) = 51$

$255 \times 3 = 765$ ✓

$102 \div 2$ ✓

$867 = 255.3 + 102$

$255 = 102.2 + 51$ ✓

$102 = 51.2 + 0$ ← ×

$51 = 255 - 102.2$

$= 255 - 2\{867 - 255.3\}$

$= 1.255 - 2.867 + 255.6$

$= 7.255 + 867(-2)$

$= 255x + 867y$

$x = 7, \quad y = -2$

Example 7 : Find the HCF of 96 and 404 by the prime factorisation method. Hence, find their LCM.

Solution : The prime factorisation of 96 and 404 gives :

2. Find the LCM and HCF of the following pairs of integers and verify that LCM × HCF = product of the two numbers.

(i) 26 and 91 (ii) 510 and 92 (iii) 336 and 54

3. Find the LCM and HCF of the following integers by applying the prime factorisation method.

(i) 12, 15 and 21 (ii) 17, 23 and 29 (iii) 8, 9 and 25

4. Given that HCF (306, 657) = 9, find LCM (306, 657).

H.W

L.C.M (306, 657) = 22338

Find the g.c.d of 414 and 662 by Euclidean algo. and write g.c.d as a L.C. of given numbers.

(a) 3 ✗ (b) 10 ✗ (c) 2 ✓ (d) 8 ✗

$d = g.c.d(a, b)$

$d \mid a, \quad d \mid b$

414 | 662 | 1
414

248 | 414 | 1
248

166 | 248 | 1
166

82 | 166 | 2
164

2 | 82 | 41
82
✗

$662 = 414.1 + 248$

$414 = 248.1 + 166$

$248 = 166.1 + 82$

$166 = 82.2 + 2$ ✓

$82 = 2.41 + 0$ ✗

$2 = 166 - 82.2$

$= 166 - \{248 - 166.1\}2$

$= 1.166 - 248.2 + 166.2$

$= 3.166 - 2.248$

$= 3\{414 - 248.1\} - 248$

$= 3.414 - 248.3 - 248$

$= 3.414 - 4.248$

$662 = 414.1 + 248$

$= 3.414 - 4\{662 - 414.1\}$

$= 3.414 - 4.662 + 4.414$

$= 7.414 - 4.662$

$= 414x + 662(y)$

$x = 7, \quad y = -4.$

Q. g.c.d (64, 48) and write g.c.d as L.C. of given number find the values of Bezout's coefficient.

g.c.d: (a) 8 (b) 16 (c) 32 (d) 48

Q. Find the G.C.D of the following pairs using Euclidean algo.

(i) (1048, 2046)

(ii) (625, 117)

(iii) (325, 115)

Two number are called coprime no. if H.C.F of these nos is 1

(5, 13) = 1 5, 13 are coprime nos

(4, 9) = 1 these are coprime nos.

(4, 8) = 4 ≠ 1 4 and 8 are not coprime nos.

— × —

Q Find H.C.F and L.C.M of 16 and 20 using prime factorization method.

$16 = 2\times2\times2\times2 = 2^4 \cdot 5^0$

$20 = 2\times2\times5 = 2^2 \cdot 5^1$

2	16
2	8
2	4
2	2
	1

2	20
2	10
5	5
	1

$H.C.F(16,20) = 2^{\min(2,4)}\ 5^{\min(0,1)}$

$= 2^2 \cdot 5^0 = 4\times1 = 4$

$L.C.M(16,20) = 2^{\max(4,2)}\ 5^{\max(0,1)} = 2^4\ 5^1 = 16\times5 = 80$

Product of nos $= 20\times16 = 320$ (Product of nos = L.C.M × H.C.F)

L.C.M × H.C.F $= 80\times4 = 320$

Q Find the H.C.F and the L.C.M of 24 and 36 also verify that Products of nos = L.C.M × H.C.F.

$24 = 2^3\times3^1$

$36 = 2^2\times3^2$

2	24
2	12
2	6
3	3
	1

2	36
2	18
3	9
3	3
	1

$H.C.F(24,36) = 2^{\min(3,2)}\ 3^{\min(1,2)}$

$= 2^2 \cdot 3^1 = 4\times3 = 12$

$L.C.M(24,36) = 2^{\max(3,2)}\ 3^{\max(1,2)} = 2^3 \cdot 3^2 = 8\times9 = 72$

Product of nos $= 24\times36 = 864$

H.C.F × L.C.M $= 12\times72 = 864$.

Q Check that 101 is a prime no or not.

$\lfloor 2 \rfloor 101 \rfloor$

Ψ

$100 < 101 < 121$

$\sqrt{100} < \sqrt{101} < \sqrt{121}$

$10 < \sqrt{101} < 11$

write all prime no's less than 10

2, 3, 5, 7

$2 \nmid 101$

$3 \nmid 101$

$5 \nmid 101$

$7 \nmid 101$

101 is a prime no

—X—

Check that 143 is a prime no or not

$121 < 143 < 144$

$\sqrt{121} < \sqrt{143} < \sqrt{144}$

$11 < \sqrt{143} < 12$

$2 \nmid 143$

$3 \nmid 143$

$5 \nmid 143$

$7 \nmid 143$

$11 \mid 143$

prime Nos less than or equal to 11 are

2, 3, 5, 7, 11

we conclude that 143 is not a prime no.

Definition of inverse of a number under mod m.

A no $\bar{a}$ is called inverse of a if

$a\bar{a} \equiv 1 \pmod{m}$ → (1)

$a \equiv b \pmod{m}$

$m \mid a\bar{a} - 1$

$(m \mid a-b)$

$\exists$ Some integer k s.t

$\exists$ Some integer k s.t

$$a\bar{a} - 1 = mk$$

or

$$a(\bar{a}) + m(-k) = 1$$

Q Find the inverse of (3) (mod 7)

$a\bar{a} \equiv 1 \pmod{m}$

Sol^n Let $\bar{a}$ be the inverse of 3

$3\bar{a} \equiv 1 \pmod 7$

$7 \mid 3\bar{a} - 1$

$\bar{a} = 1$	$7 \nmid 2$ ✗
$\bar{a} = 2$	$7 \nmid 5$ ✗
$\bar{a} = 3$,	$7 \nmid 8$
$\bar{a} = 4$,	$7 \nmid 11$
$\bar{a} = 5$	$7 \mid 14$ ✓

5 is in the inverse of 3 (mod 7)

Alter: Find the inverse of 3 (mod 7)

$$7 = 3 \times 2 + 1 \rightarrow (1)$$

$$3 = 1 \times 3 + 0 \rightarrow (2)*$$

from (1)

$7 = 3 \times 2 + 1$

$7 - 3 \times 2 = 1$

$7 \cdot 1 + 3(-2) = 1$ ✓

$$\begin{array}{r|l|r} 3 & 7 & 2 \\ & 6 & \\ \hline \rightarrow & 1 \;|\; 3 & 3 \\ & 3 & \\ \hline & x & \end{array}$$

$a\bar{a} + m(-k) = 1$

-2 is the inverse of 3 (mod 7)

$-2+7=5$

-2 is the inverse of $3 \pmod 7$

5 is the inverse of $3 \pmod 7$

Solve linear congruence.

Solve the linear congruence.

$$3x \equiv 4 \pmod 7$$

Soln $\quad 3x \equiv 4 \pmod 7$

$$7 \mid (3x-4)$$

if $x=1$,	$7 \nmid -1$ X
if $x=2$,	$7 \nmid 2$ X
if $x=3$	$7 \nmid 5$ X
if $x=4$	$7 \nmid 8$ X
if $x=5$	$7 \nmid 11$ X
if $x=6$	$7 \mid 14$ ✓

$x=6$ is the soln of the Problem.

$$[6] = \{ \ldots\ldots -8, -1, 6, 13, 20, 27, \ldots \}$$

Soln $\quad 3x \equiv 4 \pmod 5$

$x = 3$ Satisfies the above Congruence.

$[3] = \{ \ldots\ldots -12, -7, -2, 3, 8, 13, \ldots\ldots \}$

Chinese remainder Theorem.

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively coprime number and let $a_1, a_2, \ldots\ldots, a_n$ are arbitrary integers the the system of congruences.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_n \pmod{m_n}$$

has a unique Soln

$$x \equiv M_1 a_1 y_1 + M_2 a_2 y_2 + \ldots\ldots + M_n a_n y_n \pmod{m}$$

Where $m = m_1 \cdot m_2 \ldots\ldots, m_n$

Consider $x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x \equiv a_3 \pmod{m_3}$

$(m_1, m_2) = 1$, $(m_2, m_3) = 1$, $(m_3, m_1) = 1$

$M = m_1 m_2 m_3$

$M_1 = \frac{M}{m_1} = \frac{m_1 m_2 m_3}{m_1} = m_2 m_3$

$M_2 = \frac{M}{m_2} = m_1 m_3$

$M_3 = \frac{M}{m_3} = m_1 m_2$

Form new congruences

$M_1 y_1 \equiv 1 \pmod{m_1}$

$M_2 y_2 \equiv 1 \pmod{m_2}$

$M_3 y_3 \equiv 1 \pmod{m_3}$

$x \equiv M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3 \pmod{m}$

This gives us the answer of the Problem.

(a) 21 ✗ (b) 22 ✗ (c) 23 ✓ (d) 24

Q $x \equiv 2 \pmod 3$ ✓
$x \equiv 3 \pmod 5$ ✓
$x \equiv 2 \pmod 7$ ✓

$a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$

$(m_1, m_2) = (3, 5) = 1$

$(m_2, m_3) = (5, 7) = 1$

$(m_3, m_1) = (7, 3) = 1$

m_1, m_2, m_3 are pairwise coprime nos.

$M = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_1 y_1 \equiv 1 \pmod{m_1}$

$35 y_1 \equiv 1 \pmod 3$ ✓

$\therefore y_1 = 2$ is the soln of the congruence.

$M_2 y_2 \equiv 1 \pmod{m_2}$

$21 y_2 \equiv 1 \pmod 5$

$y_2 = 1$ is the soln.

$3 \mid 35$ (11) $3 \mid 70$ (23) $7 \mid 21$ (3)

$21 y_2 \equiv 1 \pmod 5$

$y_2 = 1$ is the soln.

$5 \overline{)21} \; 4$ (20, 1)

$x \equiv M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3 \pmod m$

$M_3 y_3 \equiv 1 \pmod{m_3}$

$15 y_3 \equiv 1 \pmod 7$

$= (35)(2)(2) + 21(3)(1) + 15(2)(1) \pmod{105}$

$y_3 = 1$ is the soln.

$= 140 + 63 + 30 \pmod{105}$

$= 233 \pmod{105}$

$105 \overline{)233} \; 2$ (210, 23)

$x \equiv 23 \pmod{105}$

$203 + 30 = 233$

23 is the soln of the given congruence.

Q $x \equiv 2 \pmod 3, \quad x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 5$

$a_1 = 2, \quad a_2 = 1, \quad a_3 = 3$

$m_1 = 3, \quad m_2 = 4, \quad m_3 = 5$

$M = m_1 m_2 m_3$

$= 3.4.5 = 60$

$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$

$M_3 = \frac{M}{m_3} = \frac{60}{5} = 12$

$M_1 y_1 \equiv 1 \pmod{m_1}$

$20 y_1 \equiv 1 \pmod 3$

$y_1 = 2$ is the soln

$M_2 y_2 \equiv 1 \pmod{m_2}$

$15 y_2 \equiv 1 \pmod 4$

$y_2 = 3$ is the soln.

$12 y_3 \equiv 1 \pmod{m_3}$

$12 y_3 \equiv 1 \pmod 5$

$y_3 = 1$ is the soln.

$3 \overline{)40} \; 13$ (39, 1)

$x \equiv M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3 \pmod m$

$= 20(2)(2) + 15(1)(3) + 12(3)(3) \pmod{60}$

$= 80 + 45 + 108 \pmod{60}$

$\equiv 233 \pmod{60}$

$x \equiv 53 \pmod{60}$

$108 + 80 + 45 = 233$

Q $x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

Solve the congruences with the help of Chinese remainder theorem

$x \equiv 5 \pmod 6$ ✓

$x \equiv 3 \pmod{10}$ ✓

$x \equiv 8 \pmod{15}$ ✓

$6 = 3 \times 2$ ✓ ✓

$10 = 2 \times 5$

$15 = 3 \times 5$

$(6, 10) = 2 \neq 1$

∴ As such Chinese remainder theorem is not applicable.

① $x \equiv 5 \pmod 3$, $x \equiv 2 \pmod 3$

$x \equiv 5 \pmod 2$, $x \equiv 1 \pmod 2$ → ①

② $x \equiv 3 \pmod 2$, $x \equiv 1 \pmod 2$

$x \equiv 3 \pmod 5$, $x \equiv 3 \pmod 5$ → ②

$x \equiv 8 \pmod 3$, $x \equiv 2 \pmod 3$

$x \equiv 8 \pmod 5$, $x \equiv 3 \pmod 5$ → ③

$x \equiv 2 \pmod 3$ ✓

$x \equiv 1 \pmod 2$ ✓

$x \equiv 3 \pmod 5$ ✓

$a_1 = 2, \quad a_2 = 1, \quad a_3 = 3$

$m_1 = 3, \quad m_2 = 2, \quad m_3 = 5$

$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 2 \cdot 5 = 30$

$M_1 = \frac{m}{m_1} = \frac{30}{3} = 10$

$M_2 = \frac{m}{m_2} = \frac{30}{2} = 15$ ✓

$M_1 y_1 \equiv 1 \pmod{m_1}$

$10 y_1 \equiv 1 \pmod 3$

$y_1 = 1$ is the soln.

$M_2 y_2 \equiv 1 \pmod{m_2}$

$15 y_2 \equiv 1 \pmod 2$

$y_2 = 1$ is the soln.

$M_3 y_3 \equiv 1 \pmod{m_3}$

$y_3 \equiv 1 \pmod 5$

$x \equiv M_1 a_1 y_1 + M_2 a_2 y_2 + M_3 a_3 y_3 \bmod m$

$= 10(2)(1) + 15(1)(1) + 6.3(1) \pmod{30}$

$= (20 + 15 + 18) \pmod{30}$

$= 53 \pmod{30}$

$= 23 \pmod{30}$

$M_2 = \frac{m}{m_2} = \frac{30}{2} = 15$ ✓

$M_3 = \frac{m}{m_3} = \frac{30}{5} = 6$

$\cdots 3\ y_3 \equiv 1 \pmod{m_3}$

$y_3 \equiv 1 \pmod 5$

$y_3 = 1$ is the Soln.

Q $x \equiv 7 \pmod 9$ ✓

$x \equiv 4 \pmod{12}$

$x \equiv 16 \pmod{21}$

$9 = 3^2$

$12 = 3 \times 4$ ✓

$21 = 3 \times 7$ ✓

$x \equiv 7 \pmod 9 \longrightarrow (1)$

$x \equiv 4 \pmod 4$, $x \equiv 0 \pmod 4 \rightarrow (2)$

$x \equiv 16 \pmod 7$, $x \equiv 2 \pmod 7 \rightarrow (3)$

$x \equiv 7 \pmod 9$

$x \equiv 0 \pmod 4$

$x \equiv 2 \pmod 7$