CHINESE REMAINDER THEOREM :- (CRT)

We are given two arrays num[0.... k-1] and rem[0.... k-1]. In num[0.... k-1], every pair is coprime (gcd for every pair is 1). We need to find minimum positive number 'x' such that:

$$
\begin{aligned}
x \,\%\, num[0] &= rem[0], \\
x \,\%\, num[1] &= rem[1], \\
&\vdots \\
x \,\%\, num[k-1] &= rem[k-1]
\end{aligned}
$$

Basically, we are given 'k' numbers which are pairwise Co-prime, and given remainders of these numbers when an unknown number 'x' is divided by them. We need to find the minimum possible value of x that produces given remainders.

Eg:- I/P: num[ ] = {5, 7} , rem[ ] = {1, 3}

O/P: 31

Explanation:

31 is the smallest number such that:

(1) When we divide it by 5, we get remainder 1.

(2) " " " " " 7, " " " 3.

* Chinese Remainder Theorem states that there always exists an x that satisfies given Congruences. (Chinese Remainder Theorem expressed in term of Congruences)

Def.4 :-

This may be stated as follows in term of Congruences : If the n_i are pairwise Co-prime, and if $a_1, \ldots, a_k$ are any integers, then there exists an integer x such that :

$$x \equiv a_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k};$$

and any two such x are congruent mudolo N.

let num[0], num[1] ... num[k-1] be positive integers that are pairwise coprime. Then, for any given sequence of integers rem[0], rem[1] .... rem[k-1], There exists an integer 'x' solving the following system of simultaneous congruences.

$$x \equiv rem[0] \pmod{num[0]}$$
$$\vdots$$
$$x \equiv rem[k-1] \pmod{num[k-1]}$$

Furthermore, all solutions 'x' of this system are congruent modulo the product,

Prod = num[0] * num[1] * .... num[k-1],

Hence

$$x \equiv y \pmod{num[i]}, \quad 0 \le i \le k-1$$
$$\iff$$
$$x \equiv y \pmod{prod}$$

imp. 15 MM

Q ⇒ Given two array num[0...k-1] & rem[0...k-1]. In num[0....k-1], every pair is co-prime (gcd for every pair is 1). Find the minimum positive number x for the following inputs with the help of Chinese Remainder Theorem.

a) num[] = {5, 7} , rem[] = {1, 3}

b) num[] = {3, 4, 5} , rem[] = {2, 3, 1}

Sol.ⁿ ⇒

a)

* Def.ⁿ ⇒ $x \equiv rem[\,]^{a} \pmod{num[\,]^{m}}$

$x \equiv rem[0] \pmod{num[0]}$ | $x \equiv rem[1] \pmod{num[1]}$

$x = 1 \pmod 5$ | $x \equiv 3 \pmod 7$

Check → gcd(5,7) = 1

let

$a_1 = 1$ | $m_1 = 5$

$a_2 = 3$ | $m_2 = 7$

Steps :→ formula 2

(i) $M = m_1 * m_2 = 5 * 7 = 35$

(ii) formula → $M_1 = \frac{M}{m_1} = \frac{35}{5} = 7$

$M_2 = \frac{M}{m_2} = \frac{35}{7} = 5$

(iii) Now formula → $x = (a_1 M_1 Y_1 + a_2 M_2 Y_2) \bmod M$ ——— (A)

→

Now find value of y_1 & y_2 :-

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

$7 y_1 \equiv 1 \pmod 5$

$2 y_1 \equiv 1 \pmod 5$

Multiply by 3 both side ⟸

$3(2 y_1 \equiv 1 \pmod 5)$

$6 y_1 \equiv 3 \pmod 5$

$1 y_1 \equiv 3 \pmod 5$

$\boxed{y_1 \equiv 3}$

* Multiple by 3 ∵ we have to find remainder = 1 i.e. $6 \% 5 = 1$ ⟸ (1)

$\therefore 1 y_1 = 3 \pmod 5$

$\therefore y_1 = 3$

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

$5 y_2 \equiv 1 \pmod 7$

$3*(5 y_2 \equiv 1 \pmod 7)$

$15 y_2 \equiv 3 \pmod 7$

$1 y_2 \equiv 3 \pmod 7$

$\boxed{y_2 \equiv 3}$

Now $\Rightarrow$ $x = (a_1 M_1 y_1 + a_2 M_2 y_2) \bmod M$

(A) $\Rightarrow$ $= (1*7*3 + 3*5*3) \bmod 35$

$= (21 + 45) \bmod 35$

$= 66 \bmod 35$

$\Rightarrow$ (3) Ans. ← Smallest No.

Also, $x = 31 \pmod{35}$

$\boxed{x = 31 + 35K}$ is also the solution.

where $K = 0, 1, 2, \ldots$

Pattern recognition is the science for observing, distinguishing the patterns of ...

(b) num[] = {3,4,5} , rem[] = {2, 3, 1}

Solution →

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 4$

$x \equiv 1 \bmod 5$

check → gcd{3,4,5} = 1 ✓

$a_1 = 2 \quad m_1 = 3$

$a_2 = 3 \quad m_2 = 4$

$a_3 = 1 \quad m_3 = 5$

Step 1:- $M = m_1 \times m_2 \times m_3 = 3 * 4 * 05 = 60$

Step 2:- $M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

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

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

Step 3:- $\boxed{x = (a_1 M_1 Y_1 + a_2 M_2 Y_2 + a_3 M_3 Y_3) \bmod M}$ formula.

Firstly find the value of Y_1, Y_2 & Y_3 :

(i) $\boxed{M_1 Y_1 \equiv 1 \pmod{m_1}}$ formula

$\Rightarrow 20 Y_1 \equiv 1 \pmod 3$

$Y_1 \equiv 1 \pmod{20}$

$\boxed{Y_1 = 1}$

(ii) $M_2 Y_2 \equiv 1 \pmod{m_2}$

$\Rightarrow 15 Y_2 \equiv 1 \pmod{}$

Pattern Recognition

Pattern recognition deals with identifying a pattern and confirming it again. In general, a pattern can be a fingerprint image, a handwritten cursive word, a human face, a speech signal, a bar code, or a web page on the Internet.

The individual patterns are often grouped into various categories based on their properties. When the patterns of same properties are grouped together, the resultant group is also a pattern, which is often called a pattern class.

Pattern recognition is the science for observing, distinguishing the patterns of in-

$\Rightarrow$ $2o\ y_1 \equiv 1 \pmod 3$

$\downarrow (2o \times 3)$

$2\ y_1 \equiv 1 \pmod 3$

$5\times$ $[2\ y_1 \equiv 1 \pmod 3]$

$10\ y_1 \equiv 05 \pmod 3$

$\downarrow (10 \times 3)$

$1\ y_1 \equiv 05 \pmod 3$

$\boxed{y_1 \equiv 5}$

(ii) $M_2\ y_2 \equiv 1 \pmod{m_2}$

$\Rightarrow$ $15\ y_2 \equiv 1 \pmod 4$

$\downarrow 15 \times 4$

$3\times$ $[3\ y_2 \equiv 1 \pmod 4]$

$9\ y_2 \equiv 3 \pmod 4$

$\downarrow 9 \times 4$

$1\ y_2 \equiv 3 \pmod 4$

$\boxed{y_2 \equiv 3}$

(iii) $M_3\ y_3 \equiv 1 \pmod{m_3}$

$\Rightarrow$ $12\ y_3 \equiv 1 \pmod 5$

$\downarrow 12 \times 5$

$2\ y_3 \equiv 1 \pmod 5$

$\longrightarrow$

Pattern Recognition

Pattern recognition deals with identifying a pattern and confirming it again. In general, a pattern can be a fingerprint image, a handwritten cursive word, a human face, a speech signal, a bar code, or a web page on the Internet.

The individual patterns are often grouped into various categories based on their properties. When the patterns of same properties are grouped together, the resultant group is also a pattern, which is often called a pattern class.

Pattern recognition is the science for observing, distinguishing the patterns of

$$3 \times \left[2 Y_3 \equiv 1 \pmod 5 \right]$$

$$6 Y_3 \equiv 3 \pmod 5$$

$\downarrow 6 \times 5$

$$1 Y_3 \equiv 3 \pmod 5$$

$$\boxed{Y_3 \equiv 3}$$

Now,

$$x = (a_1 M_1 Y_1 + a_2 M_2 Y_2 + a_3 M_3 Y_3) \bmod M$$

$$= (2 \times 20 \times 5 + 3 \times 15 \times 3 + 1 \times 12 \times 3) \bmod 60$$

$$= (200 + 135 + 36) \bmod 60$$

$$= 371 \bmod 60$$

$x = (11)$ dus. ← minimum/smallest value of x

Also $\Rightarrow$ $x = 11 \pmod{60}$

or

$\boxed{x = 11 + 60K}$ is also the solution.

where $K = 0, 1, 2, 3 \ldots$

Pattern Recognition

Pattern recognition deals with identifying a pattern and confirming it again. In general, a pattern can be a fingerprint image, a handwritten cursive word, a human face, a speech signal, a bar code, or a web page on the Internet.

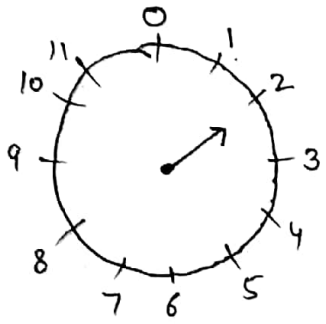
The individual patterns are often grouped into various categories based on their properties. When the patterns of same properties are grouped together, the resultant group is also a pattern, which is often called a pattern class.

Pattern recognition is the science for observing, distinguishing the patterns ... making correct decisions about the patterns or pattern cl...

Modulo Arithmetic ..... Continue.....

How can modulus be visualized using clocks?

Eg:-A) Modulo 12 addition : [only 1 hr-hand is use in this clock]

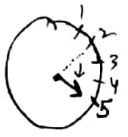


① Modulo 12 is easy to visualise using this clock

② we only need an "Hour Hand"

Let Currently Hour Hand Point to No. = 2

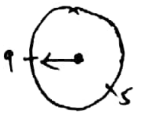
mod 12 :-
Remainder ⇒
0, 1, 2, 3 11
draw on clock



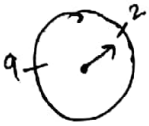
$2 + 3 \equiv 5 \pmod{12}$

(≡ : Congruent to)

let



$5 + 4 \equiv 9 \pmod{12}$



$9 + 5 \equiv 2 \pmod{12}$

$2 + 12 \equiv 2 \pmod{12}$

i.e.

$14 \equiv 2 \pmod{12}$

Pattern Recognition

Pattern recognition deals with identifying a pattern and confirming it again. In general, a pattern can be a fingerprint image, a handwritten cursive word, a human face, a speech signal, a bar code, or a web page on the Internet.

The individual patterns are often grouped into various categories based on their properties. When the patterns of same properties are grouped together, the resultant group is also a pattern, which is often called a pattern class.

Pattern recognition is the science [illegible]
making correct

$2+30 \equiv 8 \pmod{12}$

i.e. $32 \equiv 8 \pmod{12}$

$8+5 \equiv 1 \pmod{12}$

$29+72 \equiv 5+0 \pmod{12}$

$\equiv 5 \pmod{12}$

$\because \begin{cases} 29 \equiv 5 \pmod{12} \\ 72 \equiv 0 \pmod{12} \end{cases}$

or

$29+72 \equiv 5 \pmod{12}$

$101 \equiv 5 \pmod{12}$

$\because 101 = 8 \times 12 + 5$

IIly

$243+85 \equiv (3+1) \bmod 12$

$328 \equiv 4 \pmod{12}$

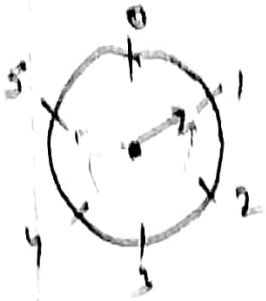
$243 \equiv 3 \pmod{12}$

$85 \equiv 1 \pmod{12}$

Eg:- 8) **Modulo Subtraction :-**

Modulo 6 Subtraction :- (This use Anticlockwise direction)

mod 6 → Remainder = 0, 1, 2, - - - 5



$5 - 4 \equiv 1 \mod 6$

$4 - 5 \equiv 5 \mod 6$