CS 2051 03/16

CRT Examples

Solve the system:

$x \equiv 3 \pmod 3$
$x \equiv 4 \pmod 5$
$x \equiv 6 \pmod 7$

Recall: the unique solution (mod 3·5·7 = 105) is

$\Rightarrow x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{105}$

where $a_1 = 1$, $M_1 = 35 = 5 \cdot 7$, $y_1 =$
$a_2 = 4$, $M_2 = 21 = 3 \cdot 7$, $y_2 =$
$a_3 = 6$, $M_3 = 15 = 3 \cdot 5$, $y_3 =$

Computing y_1, y_2, y_3:

We have $M_1 y_1 \equiv 1 \pmod{m_1}$ OR
$35 y_1 \equiv 1 \pmod 3$
$2 y_1 \equiv 1 \pmod 3 \Rightarrow \boxed{y_1 = 2}$

For $M_2 y_2 \equiv 1 \pmod{m_2}$
$21 y_2 \equiv 1 \pmod 5$
$y_2 \equiv 1 \pmod 5 \Rightarrow \boxed{y_2 = 1}$

Lastly, $M_3 y_3 \equiv 1 \pmod{m_3}$
$15 y_3 \equiv 1 \pmod 7$
$y_3 \equiv 1 \pmod 7 \Rightarrow \boxed{y_3 = 1}$

Back to our formula for x:

$x \equiv 1 \cdot 35 \cdot 2 + 4 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1 \pmod{105}$
$\equiv 70 + 84 + 90 \pmod{105}$
$\equiv 244 \pmod{105}$
$\equiv 34 \pmod{105}$

This is the only solution of the system in the set $\{0, 1, 2, \ldots, 104\}$ is $\boxed{34}$ ∎

∗ Second approach:

(1) $x \equiv 1 \pmod 3$
(2) $x \equiv 4 \pmod 5$
(3) $x \equiv 6 \pmod 7$

From (3): $\boxed{x = 7k + 6, k \in \mathbb{Z}}$

Plug in on (2):

$7k + 6 \equiv 4 \pmod 5$
$2k + 1 \equiv 4 \pmod 5$
$2k \equiv 3 \pmod 5$

We can see that $k \equiv 4 \pmod 5$ is a solution. OR

$\boxed{k = 5j + 4 \quad j \in \mathbb{Z}}$

Now $x = 7k + 6 = 7(5j + 4) + 6$

$\boxed{x = 35j + 34}$

Back to (1):

$35j + 34 \equiv 1 \pmod 3$ OR
$2j + \cancel{1} \equiv \cancel{1} \pmod 3$
$\equiv 0 \pmod 3$

i.e. $\boxed{j = 3\ell}$, $\ell \in \mathbb{Z}$.

Finally $x = 35j + 34$
$= 35(3\ell) + 34$
$= 105\ell + 34$, $\ell \in \mathbb{Z}$.

Unique sol (mod 105).

Example 2: A treasure has N gold coins.

- If the coins are divided equally among 6 pirates, 4 coins are left over.
- If the coins are divided equally among 5 pirates, 3 coins are left over.

The treasure has the minimum number of coins with these conditions.

How many coins are left over if equally divided among seven pirates?

Sol.

(1) $N \equiv 4 \pmod 6$ % when we divide N 6 equal groups there are 4 coins left!!!
(2) $N \equiv 3 \pmod 5$ % same analysis!

Want: $N \equiv ? \pmod 7$

From (1), $N = 6k + 4$ $k \in \mathbb{Z}$
In (2) $6k + 4 \equiv 3 \pmod 5$ OR
$k \equiv -1 \pmod 5 \Rightarrow k = 5\ell - 1$ ($\ell \in \mathbb{Z}$)

Then $N = 6(5\ell - 1) + 4 = 30\ell - 2$, $\ell \in \mathbb{Z}$.

Note (i) $N > 0$

(ii) If $\ell \leq 0$ then $N < 0$ because
$\rightarrow 30\ell \leq 0$ and
$N = 30\ell - 2 \leq -2 < 0$.

(iii) For $\ell = 1$: $N = 28$

From (ii)-(iii), $N = 28$ is the smallest positive solution, which is what we need!!!

$N \equiv 0 \pmod 7$

Another way to check $N = 28$ is the solution:
By CRT, the solution is unique (mod 30) OR
There is a unique number from the set $\{0, 1, 2, \ldots, 29\}$ solution to our system. We conclude that is the smallest positive integer solution!

Euler's Thm

Recall: Fermat's Thm
If $p \geq 3$ is prime and $\gcd(a, p) = 1$ then
$a^{p-1} \equiv 1 \pmod p$

Euler's Thm

$\varphi(N) = \left| \{ 1 \leq a \leq N-1 \mid \gcd(a, N) = 1 \} \right|$

Note $\varphi(N) \leq N - 1$, in particular $\varphi(p) = p - 1$ when p is prime.

(T) If $\gcd(a, N) = 1$: $a^{\varphi(N)} \equiv 1 \pmod N$

Proposition: If $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i are primes $\alpha_i \geq 0$ are natural numbers.

$$\boxed{\text{then } \varphi(N) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)}$$

Note: $N = p$ is prime means $\alpha_1 = 1$ and
$\varphi(N) = p^{1-1}(p-1) = p - 1$.

$N = 12 = 2^2 \cdot 3$ then $\varphi(12) = 2^{2-1}(2-1)(3-1)$
$= 2 \cdot 1 \cdot 2$
$= 4$

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Example: Prove $a_1, a_2, \ldots, a_{2022}$ consecutive natural numbers, such that each a_i is multiple of a square (i.e. $\exists d \in \mathbb{Z}$: d^2 / a_i $\forall i$)

Proof: Let $p_1, p_2, \ldots, p_{2022}$ be prime numbers.
Let x be a solution of ∗

$x \equiv -1 \pmod{p_1^2}$
$x \equiv -2 \pmod{p_2^2}$
$\vdots$
$x \equiv -2022 \pmod{p_{2022}^2}$

(∗) Sol exists because of CRT!!!

This translates into:

$p_1^2 / x + 1$
$p_2^2 / x + 2$
$\vdots$
$p_k^2 / x + k$

consecutive numbers!!! ∎

HAVE A GREAT BREAK!!! ☺