Search Member List Calendar Help

Hello There, Guest! (Login — Register) **Current time:** 02-19-2010, 02:14 PM

OMath! / Math Forums 数学讨论 / Number Theory / **Chinese Remainder Theory**

Thread Rating: NEW REPLY

Chinese Remainder Theory Threaded Mode | Linear Mode

02-17-2010, 03:09 PM (This post was last modified: Yesterday 12:51 AM by elim.) **Post: #1**

elim
Junior Member

Posts: 6
Joined: Feb 2010
Reputation: **0**

Chinese Remainder Theory

The theorem statement: $((n_i, n_j) = 1, \quad 1 <= i < j <= k) \Rightarrow$

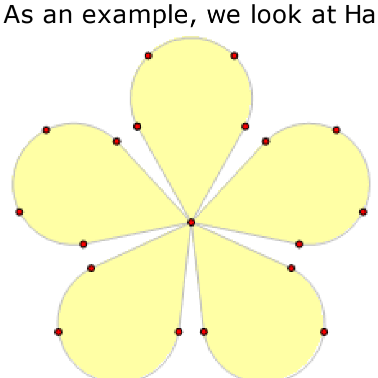
$$\forall(a_1, \cdots, a_k) \in \mathbf{N}_0^k \ \ \exists x_0 \in \mathbf{N}_0 \ (x_0 \equiv a_i (\mathrm{mod}\ n_i) \quad i = 1, k) \wedge$$

$$((x \equiv a_i (\mathrm{mod}\ n_i) \quad i = 1, k) \Leftrightarrow (x \equiv x_0 (\mathrm{mod}\ n_1 \cdots n_k)))$$

Proof. Let $N = \prod_{i=1}^{k} n_i$ then $(n_i, N/n_i) = 1$ hence
$\exists s_i, t_i \in \mathbf{Z}: \quad s_i n_i + t_i(N/n_i) = 1 \quad i = 1, k$
Let $e_i = t_i(N/n_i)$, then $(e_i \equiv 0 (\mathrm{mod}\ n_j) \ \ i \neq j) \wedge (e_i \equiv 1 (\mathrm{mod}\ n_i))$
So $x_0 = \sum_{i=1}^{k} a_i e_i$ satisfies $x_0 \equiv a_i (\mathrm{mod}\ n_i) \quad i = 1, k$
Now
$(x \equiv a_i (\mathrm{mod}\ n_i) \quad i = 1, k) \Leftrightarrow (x - x_0 \equiv 0 (\mathrm{mod}\ n_i), \quad i = 1, k) \Leftrightarrow (x \equiv x_0 (\mathrm{mod}\ N))$

Q.E.D

As an example, we look at HanXing's Soldier Counting (韩信点兵)



三人同行七十稀，五树梅花廿一枝，

七子团圆正半月，除百零五便得知。

The Chinese above is a mystery poem-code of (**) below:

(**) $x \equiv 70\lfloor x \rfloor_3 + 21\lfloor x \rfloor_5 + 15\lfloor x \rfloor_7 \pmod{105} \qquad (105 = 3 \times 5 \times 7)$
Where $\lfloor x \rfloor_j = \min\{m \in \mathbb{N}_0 : j | (x - m)\}$ is the remainder of x by j.

The poem, in English sounds roughly like this to me:

Rarely you see 3 men walking together all above 70's,
But 5 and 21 surely show the beauty of plum blossoms,
7 sons' reunion expects full moon at middle month sky,
with these to a multiple of 105 you figure it out all!

Note: In Chinese lunar calendar, full moon always appears at the middle of the month. which implies number 15.

Let's say someone chose a number in mind with remainders of 3,5 and 7 respectively as:
(1) $0, 1, 1$. Then $70 \times 0 + 21 \times 1 + 15 \times 1 = 36$ hence the number in mind is $36 + 105n$ for some $n \in \mathbb{Z}$
(2) $1, 4, 0$ Then $70 \times 1 + 21 \times 4 + 15 \times 0 = 154$ hence the number in mind is $49 + 105n$ for some $n \in \mathbb{Z}$
(3) $1, 3, 4$ Then $70 \times 1 + 21 \times 3 + 15 \times 4 = 193$ hence the number in mind is $88 + 105n$ for some $n \in \mathbb{Z}$.

If we know the number's range is $[k, k + 105)$ for some $k \in \mathbb{Z}$, we then get the definite answer. So if you ask people choose a number from $[1, 100]$ and let them to provide the remainders with respect to 3,5 and 7, you know exactly what in their mind. This is quite amazing for most people.

But in US, figure out remainders is already too hard for most people... That's why we are good at complicated measure systems: Let computer figure things out.

FIND REPLY

« Next Oldest | Next Newest » Enter Keywords Search Thread

NEW REPLY

View a Printable Version
Send this Thread to a Friend
Subscribe to this thread

Forum Jump: -- Number Theory Go

Contact Us | Advisors-Online | Return to Top | Return to Content | Lite (Archive) Mode | RSS Syndication English (American) Go

Powered By MyBB, © 2002-2010 MyBB Group.