Chinese Remainder Theorem

The **Chinese Remainder Theorem** is a number theoretic result. It is one of the only theorems named for an oriental person or place, due to the closed development of mathematics in the western world.

Contents

Theorem

Formally stated, the Chinese Remainder Theorem is as follows:

Let m be relatively prime to n. Then each residue class mod mn is equal to the intersection of a unique residue class mod m and a unique residue class mod n, and the intersection of each residue class mod m with a residue class mod n is a residue class mod mn.

Simply stated:

Suppose you wish to find the least number x which leaves a remainder of:

$$\begin{aligned} y_1 &\text{ when divided by } & d_1 \\ y_2 &\text{ when divided by } & d_2 \\ &\vdots & \vdots \\ y_n &\text{ when divided by } & d_n \end{aligned}$$

such that $d_1, d_2, \ldots d_n$ are all relatively prime. Let $M = d_1 d_2 \cdots d_n$, and $b_i = \frac{M}{d_i}$. Now if the numbers a_i satisfy:

$$a_i b_i - 1 \equiv 0 \pmod{d_i}$$

for every $1 \leq i \leq n$, then a solution for x is:

$$x = \sum_{i=1}^{n} a_i b_i y_i \pmod{M}$$

Proof

If $a \equiv b \pmod{mn}$, then a and b differ by a multiple of mn, so $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. This is the first part of the theorem. The converse follows because a and b must differ by a multiple of m and n, and $\operatorname{lcm}(m, n) = mn$. This is the second part of the theorem.

Applicability

Much like the Fundamental Theorem of Arithmetic, many people seem to take this theorem for granted before they consciously turn their attention to it. Its ubiquity derives from the fact that many results can be easily proven mod (a power of a prime), and can then be generalized to mod m using the Chinese Remainder Theorem. For instance, Fermat's Little Theorem may be generalized to the Fermat-Euler Theorem in this manner.

General Case: the proof of the general case follows by induction to the above result (k-1) times.

Extended version of the theorem

Suppose one tried to divide a group of fish into $2, 3$ and 4 parts instead and found $1, 1$ and 2 fish left over, respectively. Any number with remainder 1 mod 2 must be odd and any number with remainder 2 mod 4 must be even. Thus, the number of objects must be odd and even simultaneously, which is a contradiction. Thus, there must be restrictions on the numbers $a_1, \ldots, a_n$ to ensure that at least one solution exists. It follows that:

The solution exists if and only if $a_i \equiv a_j \mod \gcd(m_i, m_j)$ *for all* i, j *where* $\gcd$ *stands for the greatest common divisor. Moreover, in the case when the problem is solvable, any two solutions differ by some common multiple of* $m_1, \ldots, m_n$. (the extended version).

See Also

- Modular arithmetic/Introduction
- Chicken McNugget Theorem

Discussion

- Here (http://www.artofproblemsolving.com/Forum/viewtopic.php?t=80124&sid=df9439496046e0ff9f97cfc644408395) is an AoPS thread in which the Chinese Remainder Theorem is discussed and implemented.

Retrieved from "http://artofproblemsolving.com/wiki/index.php?title=Chinese_Remainder_Theorem&oldid=84247"

Categories: Number theory | Theorems

Copyright © 2017 Art of Problem Solving