The Chinese Remainder Theorem

Consider

Oystein Ore mentions a puzzle with a dramatic element from *Brahma-Sphuta-Siddhanta* (Brahma's Correct System) by Brahmagupta (born 598 AD):

An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

The Chinese Remainder Theorem

Theorem: Suppose that $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers, and let $a_1, a_2, \ldots, a_r$ be integers. Then the system of congruences, $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$, has a unique solution modulo $M = m_1 \times m_2 \times \ldots \times m_r$, which is given by:

$$x \equiv a_1M_1y_1 + a_2M_2y_2 + \ldots + a_rM_ry_r \pmod{M},$$

where $M_i = M/m_i$ and $y_i \equiv (M_i)^{-1} \pmod{m_i}$ for $1 \le i \le r$.

The Chinese Remainder Theorem

Theorem: Suppose that $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers, and let $a_1, a_2, \ldots, a_r$ be integers. Then the system of congruences, $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$, has a unique solution modulo $M = m_1 \times m_2 \times \ldots \times m_r$, which is given by:

$$x \equiv a_1M_1y_1 + a_2M_2y_2 + \ldots + a_rM_ry_r \pmod{M},$$

where $M_i = M/m_i$ and $y_i \equiv (M_i)^{-1} \pmod{m_i}$ for $1 \le i \le r$.

Pf: Notice that $\gcd(M_i, m_i) = 1$ for $1 \le i \le r$. Therefore, the y_i all exist (determined easily from the extended Euclidean Algorithm). Now, notice that since $M_iy_i \equiv 1 \pmod{m_i}$, we have $a_iM_iy_i \equiv a_i \pmod{m_i}$ for $1 \le i \le r$. On the other hand, $a_iM_iy_i \equiv 0 \pmod{m_j}$ if $j \ne i$ (since $m_j \mid M_i$ in this case). Thus, we see that $x \equiv a_i \pmod{m_i}$ for $1 \le i \le r$.

If x_0 and x_1 were solutions, then we would have $x_0 - x_1 \equiv 0 \pmod{m_i}$ for all i, so $x_0 - x_1 \equiv 0 \pmod{M}$, i.e., they are the same modulo M. ❑

Example

Find the smallest multiple of 10 which has remainder 2 when divided by 3, and remainder 3 when divided by 7.

We are looking for a number which satisfies the congruences, $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 7$, $x \equiv 0 \bmod 2$ and $x \equiv 0 \bmod 5$. Since, 2, 3, 5 and 7 are all relatively prime in pairs, the Chinese Remainder Theorem tells us that there is a unique solution modulo 210 ($= 2\times3\times5\times7$). We calculate the M_i's and y_i's as follows:

$M_2 = 210/2 = 105$; $y_2 \equiv (105)^{-1} \pmod 2 = 1$

$M_3 = 210/3 = 70$; $y_3 \equiv (70)^{-1} \pmod 3 = 1$

$M_5 = 210/5 = 42$; $y_5 \equiv (42)^{-1} \pmod 5 = 3$ and

$M_7 = 210/7 = 30$; $y_7 \equiv (30)^{-1} \pmod 7 = 4$.

So, $x \equiv 0(M_2y_2) + 2(M_3y_3) + 0(M_5y_5) + 3(M_7y_7) \equiv 0 + 2(70)(1) + 0 + 3(30)(4) \equiv 140 + 360 \equiv 500 \bmod 210 \equiv \mathbf{80}$.

Broken Eggs

The number of broken eggs, x, must satisfy:

$$x \equiv 1 \bmod 2,$$
$$x \equiv 1 \bmod 3,$$
$$x \equiv 1 \bmod 4,$$
$$x \equiv 1 \bmod 5,$$
$$x \equiv 1 \bmod 6 \text{ and}$$
$$x \equiv 0 \bmod 7.$$

The first congruence says that x is odd, so we shall keep this in mind and ignore this congruence. To use our theorem, we will also omit the congruence $x \equiv 1 \bmod 6$ so that the moduli of the remaining congruences (3, 4, 5 and 7) are relatively prime in pairs.

Broken Eggs

The Chinese Remainder theorem indicates that there is a unique solution modulo 420 ($= 3 \times 4 \times 5 \times 7$), which is calculated by:

$M_3 = 420/3 = 140$ $\qquad$ $y_3 \equiv (140)^{-1} \bmod 3 = 2$

$M_4 = 420/4 = 105$ $\qquad$ $y_4 \equiv (105)^{-1} \bmod 4 = 1$

$M_5 = 420/5 = 84$ $\qquad$ $y_5 \equiv (84)^{-1} \bmod 5 = 4$

$M_7 = 420/7 = 60$ $\qquad$ $y_7 \equiv (60)^{-1} \bmod 7 = 2$

so $x \equiv 1(140)(2) + 1(105)(1) + 1(84)(4) + 0(60)(2) = 280 + 105 + 336 = 721 \bmod 420 =$ **301**.

As this value of x is odd and satisfies $x \equiv 1 \bmod 6$, it is the smallest solution of the broken eggs problem.

Notes

Remark 1: The theorem is valid in much more general situations than we have presented here.

Remark 2: The condition given is sufficient, but not necessary for a solution. Necessary and sufficient conditions exist but we are not presenting them.

Remark 3: It is purported that Sun Tsu was aware of this result in the first century A.D.