



M. F. Gilmullin, "The Chinese Remainder Theorem," *Mathematics with Mansur*, Feb. 5, 2026. [Online]. Available: <https://history-math.org/publications/hm-tt-dd2ef8a97500-en/>.

ESSAY

The Chinese Remainder Theorem

A legend about counting soldiers leads to the Chinese remainder theorem: recovering an integer from its remainders modulo pairwise coprime numbers.

Mansur Gilmullin · 05.02.2026 · EN

[Read this article on the journal website](#)



China's famous Terracotta Army: an illustration for the legend about military formations. · [Source](#)

There is a legend.

Commanders in ancient China supposedly gave a series of orders such as "Form rows of 7!", "Form rows of 11!", and so on, observing each time how many soldiers were left in the final row. Using only those remainders, they then calculated the total number of soldiers.

In mathematical literature, the algorithm for solving such problems is called the Chinese remainder theorem, often abbreviated CRT.

The theorem has a beautiful meaning: it allows an integer to be recovered from its remainders upon division by several numbers, provided those numbers are pairwise coprime. This is a classical result of number theory that has long extended beyond “pure mathematics” into computer algebra and cryptography.

Historical background

The idea is described in arithmetic form in a treatise known as the *Sunzi Suanjing*, traditionally assigned to an early period, usually the third century CE. In the thirteenth century, the Chinese mathematician Qin Jiushao substantially generalised these methods in *Mathematical Treatise in Nine Sections* (1247), providing a systematic algorithm for solving such problems.

A problem from Sunzi’s book

“Suppose there is an unknown number of objects. When divided into threes, 2 remain; when divided into fives, 3 remain; when divided into sevens, 2 remain. How many objects are there?”

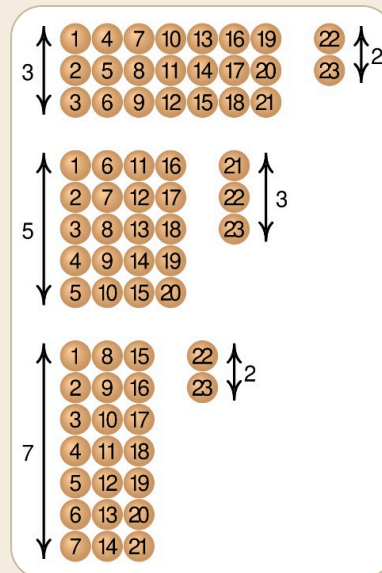
After solving this particular problem, the text gives an algorithm for the general case, with arbitrary remainders:

“Multiply the remainder upon division into threes by 70. Add the product of the remainder upon division into fives and 21, then add the product of the remainder upon division into sevens and 15. If the result is 106 or more, subtract a multiple of 105.”

Let us check our values:

$$2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 = 105 \cdot 2 + 23$$

The smallest solution is therefore 23.



Explanation of the problem solved by Sunzi's algorithm: $2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233$. · [Source](#)

Why do 70, 21 and 15 appear here? There is no magic: in modern mathematical language, they involve partial products and their modular inverses, the “building blocks” of the general algorithm.

Two elementary explanations

Method 1: combinatorial

Write out the sets of solutions to the three separate conditions. It is enough to consider numbers up to $3 \cdot 5 \cdot 7 = 105$:

$x \equiv 2 \pmod{3}$: {2, 5, 8, 11, 14, 17, 20, 23, 26, ...}

$x \equiv 3 \pmod{5}$: {3, 8, 13, 18, 23, 28, ...}

$x \equiv 2 \pmod{7}$: {2, 9, 16, 23, 30, ...}

The answer must lie in the intersection of the three sets. In our case, the smallest common number is 23. The next are 128, 233 and so on: all solutions have the form $23 + 105k$.

Method 2: algebraic

Write the conditions as equalities with integer parameters:

$$x = 2 + 3q$$

$$x = 3 + 5p$$

$$x = 2 + 7t$$

We then successively reconcile the first two equalities, followed by the resulting expression and the third:

$$\begin{aligned}
2 + 3q &= 3 + 5p \\
q &= (5p + 1)/3 = p + (2p + 1)/3 \\
2p + 1 &= 3u \\
p &= (3u - 1)/2 = u + (u - 1)/2 \\
u - 1 &= 2v \\
u &= 2v + 1 \\
x = 3 + 5p &= 3 + 5(u + v) = 3 + 5(2v + 1 + v) = 8 + 15v \\
8 + 15v &= 2 + 7t \\
t &= (15v + 6)/7 = 2v + (v + 6)/7 \\
v + 6 &= 7w \\
v &= 7w - 6 \\
t &= 2(7w - 6) + w = 15w - 12 \\
x &= 2 + 7(15w - 12) = 105w - 82 = 105(w - 1) + 23
\end{aligned}$$

The result is $x = 105(w - 1) + 23$. Thus the smallest solution is 23, and the others are obtained by adding 105.

(The parameters q, p, t, u, v, w are understood to be integers.)

General statement and algorithm

In number theory, the theorem is stated in the language of systems of linear congruences.

Let $m_1, m_2, \dots, m_k$ be pairwise coprime positive integers: $\gcd(m_i, m_j) = 1$ for any $i \neq j$.

Let $r_1, r_2, \dots, r_k$ be arbitrary integers, usually with r_i the remainder upon division by m_i . Then the system of congruences

$$x \equiv r_i \pmod{m_i}, i = 1, \dots, k$$

has a solution, and all its solutions are congruent modulo $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$.

One standard algorithm is as follows; various proofs are known:

1. Calculate the overall modulus:

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_k$$

2. Calculate the partial products for each i :

$$M_i = M/m_i$$

3. Find the inverses:

for each i , find y_i such that $M_i \cdot y_i \equiv 1 \pmod{m_i}$

(For example, use the extended Euclidean algorithm.)

4. Find a solution:

$$x = (r_1 \cdot M_1 \cdot y_1 + r_2 \cdot M_2 \cdot y_2 + \dots + r_k \cdot M_k \cdot y_k) \pmod{M}$$

For our example:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$M = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = 35$$

$$M_2 = 21$$

$$M_3 = 15$$

Find the inverses:

$$M_1 \cdot y_1 \equiv 1 \pmod{3}$$

$$35 \cdot y_1 \equiv 1 \pmod{3}$$

$$y_1 = 2$$

$$M_2 \cdot y_2 \equiv 1 \pmod{5}$$

$$21 \cdot y_2 \equiv 1 \pmod{5}$$

$$y_2 = 1$$

$$M_3 \cdot y_3 \equiv 1 \pmod{7}$$

$$15 \cdot y_3 \equiv 1 \pmod{7}$$

$$y_3 = 1$$

Then $x \equiv 233 \pmod{105}$, and $233 = 105 \cdot 2 + 23$, so $x \equiv 23 \pmod{105}$.

As you can see, every method reaches the same result, simply by a different route.

 [Mathematics with Mansur-abyy](#)