WIKIPEDIA
The Free Encyclopedia

Chinese remainder theorem

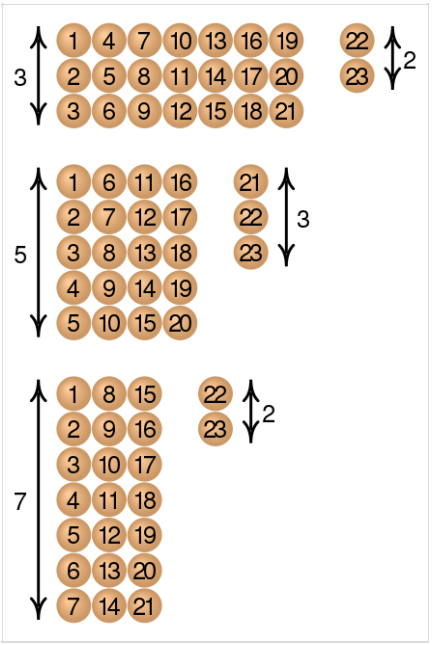
In mathematics, the **Chinese remainder theorem** states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime (no two divisors share a common factor other than 1).

For example, if we know that the remainder of n divided by 3 is 2, the remainder of n divided by 5 is 3, and the remainder of n divided by 7 is 2, then without knowing the value of n, we can determine that the remainder of n divided by 105 (the product of 3, 5, and 7) is 23. Importantly, this tells us that if n is a natural number less than 105, then 23 is the only possible value of n.

The earliest known statement of the theorem is by the Chinese mathematician Sunzi in the *Sunzi Suanjing* in the 3rd century CE.

The Chinese remainder theorem is widely used for computing with large integers, as it allows replacing a computation for which one knows a bound on the size of the result by several similar computations on small integers.

The Chinese remainder theorem (expressed in terms of congruences) is true over every principal ideal domain. It has been generalized to any ring, with a formulation involving two-sided ideals.



Sunzi's original formulation:
$x \equiv 2 \pmod 3 \equiv 3 \pmod 5$
$\equiv 2 \pmod 7$ with the solution
$x = 23 + 105k$, with k an integer

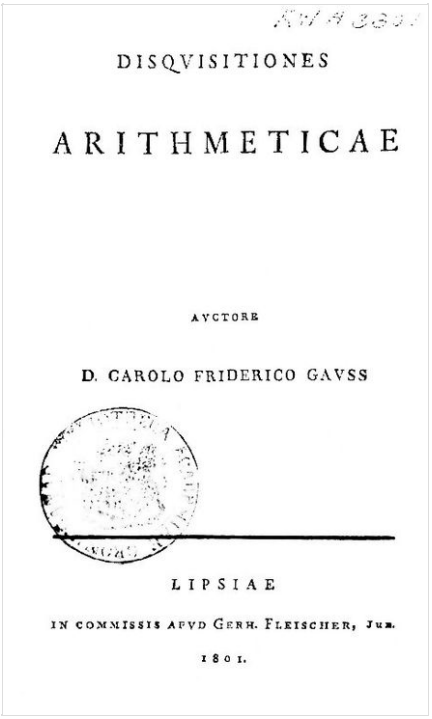
History

The earliest known statement of the theorem, as a problem with specific numbers, appears in the 3rd-century book *Sunzi Suanjing* by the Chinese mathematician Sunzi:[1]

> There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?[2]

Sunzi's work contains neither a proof nor a full algorithm.[3] What amounts to an algorithm for solving this problem was described by Aryabhata (6th century).[4] Special cases of the Chinese remainder theorem were also known to Brahmagupta (7th century), and appear in Fibonacci's Liber Abaci (1202).[5] The result was later generalized with a complete solution called *Da-yan-shu* (大衍術) in Qin Jiushao's 1247 *Mathematical Treatise in Nine Sections* [6] which was translated into English in early 19th century by British missionary Alexander Wylie.[7]

The notion of congruences was first introduced and used by Carl Friedrich Gauss in his *Disquisitiones Arithmeticae* of 1801.[9] Gauss illustrates the Chinese remainder theorem on a problem involving calendars, namely, "to find the years that have a certain period number with respect to the solar and lunar cycle and the Roman indiction."[10] Gauss introduces a procedure for solving the problem that had already been used by Leonhard Euler but was in fact an ancient method that had appeared several times.[11]


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

The Chinese remainder theorem appears in Gauss's 1801 book *Disquisitiones Arithmeticae*.[8]

Statement

Let $n_1, \ldots, n_k$ be integers greater than 1, which are often called *moduli* or *divisors*. Let us denote by N the product of the n_i.

The Chinese remainder theorem asserts that if the n_i are pairwise coprime, and if $a_1, \ldots, a_k$ are integers such that $0 \le a_i < n_i$ for every i, then there is one and only one integer x, such that $0 \le x < N$ and the remainder of the Euclidean division of x by n_i is a_i for every i.

This may be restated as follows in terms of congruences: If the n_i are pairwise coprime, and if $a_1, \ldots, a_k$ are any integers, then the system

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k}, \end{aligned}$$

has a solution, and any two solutions, say x_1 and x_2, are congruent modulo N, that is, $x_1 \equiv x_2 \pmod{N}$.[12]

In abstract algebra, the theorem is often restated as: if the n_i are pairwise coprime, the map

$$x \bmod N \mapsto (x \bmod n_1, \ldots, x \bmod n_k)$$

defines a ring isomorphism[13]

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

between the ring of integers modulo N and the direct product of the rings of integers modulo the n_i. This means that for doing a sequence of arithmetic operations in $\mathbb{Z}/N\mathbb{Z}$, one may do the same computation independently in each $\mathbb{Z}/n_i\mathbb{Z}$ and then get the result by applying the isomorphism (from the right to the left). This may be much faster than the direct computation if N and the number of operations are large. This is widely used, under the name *multi-modular computation*, for linear algebra over the integers or the rational numbers.

The theorem can also be restated in the language of combinatorics as the fact that the infinite arithmetic progressions of integers form a Helly family.[14]

Proof

The existence and the uniqueness of the solution may be proven independently. However, the first proof of existence, given below, uses this uniqueness.

Uniqueness

Suppose that x and y are both solutions to all the congruences. As x and y give the same remainder, when divided by n_i, their difference $x - y$ is a multiple of each n_i. As the n_i are pairwise coprime, their product N also divides $x - y$, and thus x and y are congruent modulo N. If x and y are supposed to be non-negative and less than N (as in the first statement of the theorem), then their difference may be a multiple of N only if $x = y$.

Existence (first proof)

The map

$$x \bmod N \mapsto (x \bmod n_1, \ldots, x \bmod n_k)$$

maps congruence classes modulo N to sequences of congruence classes modulo n_i. The proof of uniqueness shows that this map is injective. As the domain and the codomain of this map have the same number of elements, the map is also surjective, which proves the existence of the solution.

This proof is very simple but does not provide any direct way for computing a solution. Moreover, it cannot be generalized to other situations where the following proof can.

Existence (constructive proof)

Existence may be established by an explicit construction of x.[15] This construction may be split into two steps, first solving the problem in the case of two moduli, and then extending this solution to the general case by induction on the number of moduli.

Case of two moduli

We want to solve the system:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2}, \end{aligned}$$

where n_1 and n_2 are coprime.

Bézout's identity asserts the existence of two integers m_1 and m_2 such that

$$m_1 n_1 + m_2 n_2 = 1.$$

The integers m_1 and m_2 may be computed by the extended Euclidean algorithm.

A solution is given by

$$x = a_1 m_2 n_2 + a_2 m_1 n_1 .$$

Indeed,

$$\begin{aligned} x &= a_1 m_2 n_2 + a_2 m_1 n_1 \\ &= a_1(1 - m_1 n_1) + a_2 m_1 n_1 \\ &= a_1 + (a_2 - a_1) m_1 n_1, \end{aligned}$$

implying that $x \equiv a_1 \pmod{n_1}$. The second congruence is proved similarly, by exchanging the subscripts 1 and 2.

General case

Consider a sequence of congruence equations:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k}, \end{aligned}$$

where the n_i are pairwise coprime. The two first equations have a solution $a_{1,2}$ provided by the method of the previous section. The set of the solutions of these two first equations is the set of all solutions of the equation

$$x \equiv a_{1,2} \pmod{n_1 n_2}.$$

As the other n_i are coprime with $n_1 n_2$, this reduces solving the initial problem of k equations to a similar problem with $k - 1$ equations. Iterating the process, one gets eventually the solutions of the initial problem.

Existence (direct construction)

For constructing a solution, it is not necessary to make an induction on the number of moduli. However, such a direct construction involves more computation with large numbers, which makes it less efficient and less used. Nevertheless, Lagrange interpolation is a special case of this construction, applied to polynomials instead of integers.

Let $N_i = N/n_i$ be the product of all moduli but one. As the n_i are pairwise coprime, N_i and n_i are coprime. Thus Bézout's identity applies, and there exist integers M_i and m_i such that

$$M_i N_i + m_i n_i = 1.$$

A solution of the system of congruences is

$$x = \sum_{i=1}^{k} a_i M_i N_i.$$

In fact, as N_j is a multiple of n_i for $i \neq j$, we have

$$x \equiv a_i M_i N_i \equiv a_i(1 - m_i n_i) \equiv a_i \pmod{n_i},$$

for every i.

Computation