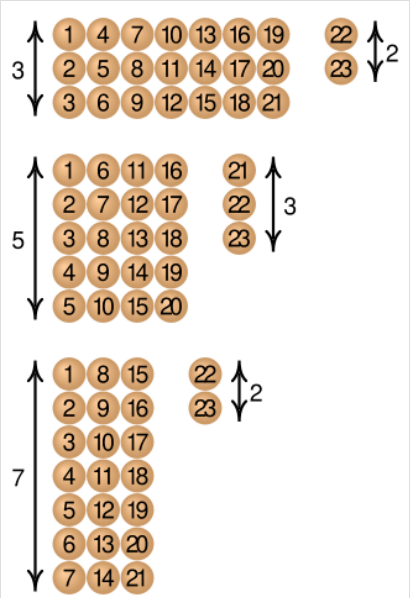
Chinese remainder theorem

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).



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

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 with no other information, 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.

It is also known as **Sunzi's theorem**, as the earliest known statement is by the Chinese mathematician Sunzi in the *Sunzi Suanjing* in the 3rd to 5th 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.

History

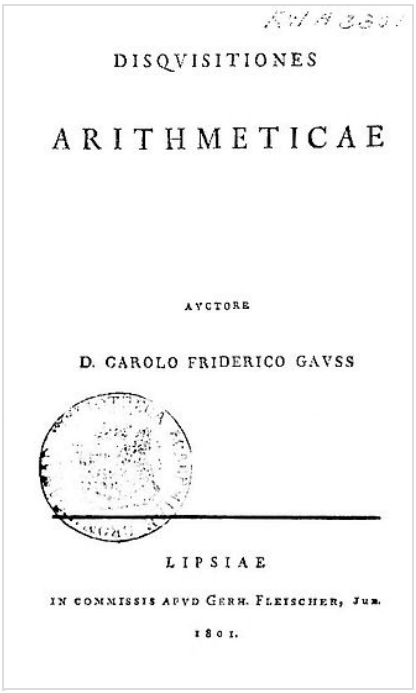
The earliest known statement of the problem appears in the 5th-century book *Sunzi Suanjing* by the Chinese mathematician Sunzi:[1]

> 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 would not be considered a theorem by modern standards; it only gives one particular problem, without showing how to solve it, much less any proof about the general case or a general algorithm for solving it.[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

Consider a system of congruences:

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

where the n_i are pairwise coprime, and let $N = n_1 n_2 \cdots n_k$. In this section several methods are described for computing the unique solution for x, such that $0 \leq x < N$, and these methods are applied on the example

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5}. \end{aligned}$$

Several methods of computation are presented. The two first ones are useful for small examples, but become very inefficient when the product $n_1 \cdots n_k$ is large. The third one uses the existence proof given in § Existence (constructive proof). It is the most convenient when the product $n_1 \cdots n_k$ is large, or for computer computation.

Systematic search

It is easy to check whether a value of x is a solution: it suffices to compute the remainder of the Euclidean division of x by each n_i. Thus, to find the solution, it suffices to check successively the integers from 0 to N until finding the solution.

Although very simple, this method is very inefficient. For the simple example considered here, 40 integers (including 0) have to be checked for finding the solution, which is 39. This is an exponential time algorithm, as the size of the input is, up to a constant factor, the number of digits of N, and the average number of operations is of the order of N.

Therefore, this method is rarely used, neither for hand-written computation nor on computers.

Search by sieving

The search of the solution may be made dramatically faster by sieving. For this method, we suppose, without loss of generality, that $0 \leq a_i < n_i$ (if it were not the case, it would suffice to replace each a_i by the remainder of its division by n_i). This implies that the solution belongs to the arithmetic progression

$$a_1, a_1 + n_1, a_1 + 2n_1, \ldots$$

By testing the values of these numbers modulo n_2, one eventually finds a solution x_2 of the two first congruences. Then the solution belongs to the arithmetic progression

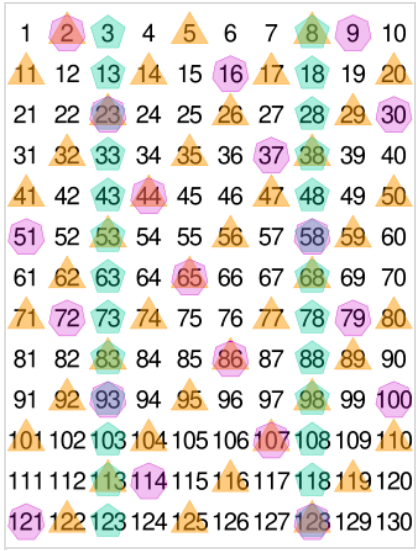
$$x_2, x_2 + n_1 n_2, x_2 + 2n_1 n_2, \ldots$$

Testing the values of these numbers modulo n_3, and continuing until every modulus has been tested eventually yields the solution.

This method is faster if the moduli have been ordered by decreasing value, that is if $n_1 > n_2 > \cdots > n_k$. For the example, this gives the following computation. We consider first the numbers that are congruent to 4 modulo 5 (the largest modulus), which are 4, 9 = 4 + 5, 14 = 9 + 5, ... For each of them, compute the remainder by 4 (the second largest modulus) until getting a number congruent to 3 modulo 4. Then one can proceed by adding 20 = 5 × 4 at each step, and computing only the remainders by 3. This gives

4 mod 4 → 0. Continue
4 + 5 = 9 mod 4 →1. Continue
9 + 5 = 14 mod 4 → 2. Continue
14 + 5 = 19 mod 4 → 3. OK, continue by considering remainders modulo 3 and adding 5 × 4 = 20 each time
19 mod 3 → 1. Continue
19 + 20 = 39 mod 3 → 0. OK, this is the result.

This method works well for hand-written computation with a product of moduli that is not too big. However, it is much slower than other methods, for very large products of moduli. Although dramatically faster than the systematic search, this method also has an exponential time complexity and is therefore not used on computers.



The smallest two solutions, 23 and 128, of the original formulation of the Chinese remainder theorem problem found using a sieve

Using the existence construction

The constructive existence proof shows that, in the case of two moduli, the solution may be obtained by the computation of the Bézout coefficients of the moduli, followed by a few multiplications, additions and reductions modulo $n_1 n_2$ (for getting a result in the interval $(0, n_1 n_2 - 1)$). As the Bézout's coefficients may be computed with the extended Euclidean algorithm, the whole computation, at most, has a quadratic time complexity of $O((s_1 + s_2)^2)$, where s_i denotes the number of digits of n_i.

For more than two moduli, the method for two moduli allows the replacement of any two congruences by a single congruence modulo the product of the moduli. Iterating this process provides eventually the solution with a complexity, which is quadratic in the number of digits of the product of all moduli. This quadratic time complexity does not depend on the order in which the moduli are regrouped. One may regroup the two first moduli, then regroup the resulting modulus with the next one, and so on. This strategy is the easiest to implement, but it also requires more computation involving large numbers.

Another strategy consists in partitioning the moduli in pairs whose product have comparable sizes (as much as possible), applying, in parallel, the method of two moduli to each pair, and iterating with a number of moduli approximatively divided by two. This method allows an easy parallelization of the algorithm. Also, if fast algorithms (that is, algorithms working in quasilinear time) are used for the basic operations, this method provides an algorithm for the whole computation that works in quasilinear time.

On the current example (which has only three moduli), both strategies are identical and work as follows.

Bézout's identity for 3 and 4 is

$$1 \times 4 + (-1) \times 3 = 1.$$

Putting this in the formula given for proving the existence gives

$$0 \times 1 \times 4 + 3 \times (-1) \times 3 = -9$$

for a solution of the two first congruences, the other solutions being obtained by adding to −9 any multiple of 3 × 4 = 12. One may continue with any of these solutions, but the solution 3 = −9 +12 is smaller (in absolute value) and thus leads probably to an easier computation

Bézout identity for 5 and 3 × 4 = 12 is

$$5 \times 5 + (-2) \times 12 = 1.$$

Applying the same formula again, we get a solution of the problem:

$$5 \times 5 \times 3 + 12 \times (-2) \times 4 = -21.$$

The other solutions are obtained by adding any multiple of 3 × 4 × 5 = 60, and the smallest positive solution is −21 + 60 = 39.

As a linear Diophantine system

The system of congruences solved by the Chinese remainder theorem may be rewritten as a system of linear Diophantine equations:

$$\begin{aligned} x &= a_1 + x_1 n_1 \\ &\vdots \\ x &= a_k + x_k n_k, \end{aligned}$$

where the unknown integers are x and the x_i. Therefore, every general method for solving such systems may be used for finding the solution of Chinese remainder theorem, such as the reduction of the matrix of the system to Smith normal form or Hermite normal form. However, as usual when using a general algorithm for a more specific problem, this approach is less efficient than the method of the preceding section, based on a direct use of Bézout's identity.

Over principal ideal domains

In § Statement, the Chinese remainder theorem has been stated in three different ways: in terms of remainders, of congruences, and of a ring isomorphism. The statement in terms of remainders does not apply, in general, to principal ideal domains, as remainders are not defined in such rings. However, the two other versions make sense over a principal ideal domain R: it suffices to replace "integer" by "element of the domain" and $\mathbb{Z}$ by R. These two versions of the theorem are true in this context, because the proofs (except for the first existence proof), are based on Euclid's lemma and Bézout's identity, which are true over every principal domain.

However, in general, the theorem is only an existence theorem and does not provide any way for computing the solution, unless one has an algorithm for computing the coefficients of Bézout's identity.

Over univariate polynomial rings and Euclidean domains

The statement in terms of remainders given in § Theorem statement cannot be generalized to any principal

ideal domain, but its generalization to Euclidean domains is straightforward. The univariate polynomials over a field is the typical example of a Euclidean domain which is not the integers. Therefore, we state the theorem for the case of the ring $R = K[X]$ for a field K. For getting the theorem for a general Euclidean domain, it suffices to replace the degree by the Euclidean function of the Euclidean domain.

The Chinese remainder theorem for polynomials is thus: Let $P_i(X)$ (the moduli) be, for $i = 1, \ldots, k$, pairwise coprime polynomials in $R = K[X]$. Let $d_i = \deg P_i$ be the degree of $P_i(X)$, and D be the sum of the d_i. If $A_i(X), \ldots, A_k(X)$ are polynomials such that $A_i(X) = 0$ or $\deg A_i < d_i$ for every i, then, there is one and only one polynomial $P(X)$, such that $\deg P < D$ and the remainder of the Euclidean division of $P(X)$ by $P_i(X)$ is $A_i(X)$ for every i.

The construction of the solution may be done as in § Existence (constructive proof) or § Existence (direct proof). However, the latter construction may be simplified by using, as follows, partial fraction decomposition instead of the extended Euclidean algorithm.

Thus, we want to find a polynomial $P(X)$, which satisfies the congruences

$$P(X) \equiv A_i(X) \pmod{P_i(X)},$$

for $i = 1, \ldots, k$.

Consider the polynomials

$$Q(X) = \prod_{i=1}^{k} P_i(X)$$
$$Q_i(X) = \frac{Q(X)}{P_i(X)}.$$

The partial fraction decomposition of $1/Q(X)$ gives k polynomials $S_i(X)$ with degrees $\deg S_i(X) < d_i$, such that

$$\frac{1}{Q(X)} = \sum_{i=1}^{k} \frac{S_i(X)}{P_i(X)},$$

and thus

$$1 = \sum_{i=1}^{k} S_i(X) Q_i(X).$$

Then a solution of the simultaneous congruence system is given by the polynomial

$$\sum_{i=1}^{k} A_i(X) S_i(X) Q_i(X).$$

In fact, we have

$$\sum_{i=1}^{k} A_i(X) S_i(X) Q_i(X) = A_i(X) + \sum_{j=1}^{k} (A_j(X) - A_i(X)) S_j(X) Q_j(X) \equiv A_i(X) \pmod{P_i(X)},$$

for $1 \leq i \leq k$.

This solution may have a degree larger than $D = \sum_{i=1}^{k} d_i$. The unique solution of degree less than D may be deduced by considering the remainder $B_i(X)$ of the Euclidean division of $A_i(X)S_i(X)$ by $P_i(X)$. This solution is

$$P(X) = \sum_{i=1}^{k} B_i(X)Q_i(X).$$

Lagrange interpolation

A special case of Chinese remainder theorem for polynomials is Lagrange interpolation. For this, consider k monic polynomials of degree one:

$$P_i(X) = X - x_i.$$

They are pairwise coprime if the x_i are all different. The remainder of the division by $P_i(X)$ of a polynomial $P(X)$ is $P(x_i)$, by the polynomial remainder theorem.

Now, let $A_1, \ldots, A_k$ be constants (polynomials of degree 0) in K. Both Lagrange interpolation and Chinese remainder theorem assert the existence of a unique polynomial $P(X)$, of degree less than k such that

$$P(x_i) = A_i,$$

for every i.

Lagrange interpolation formula is exactly the result, in this case, of the above construction of the solution. More precisely, let

$$Q(X) = \prod_{i=1}^{k} (X - x_i)$$

$$Q_i(X) = \frac{Q(X)}{X - x_i}.$$

The partial fraction decomposition of $\frac{1}{Q(X)}$ is

$$\frac{1}{Q(X)} = \sum_{i=1}^{k} \frac{1}{Q_i(x_i)(X - x_i)}.$$

In fact, reducing the right-hand side to a common denominator one gets

$$\sum_{i=1}^{k} \frac{1}{Q_i(x_i)(X - x_i)} = \frac{1}{Q(X)} \sum_{i=1}^{k} \frac{Q_i(X)}{Q_i(x_i)},$$

and the numerator is equal to one, as being a polynomial of degree less than k, which takes the value one for k different values of X.

Using the above general formula, we get the Lagrange interpolation formula:

$$P(X) = \sum_{i=1}^{k} A_i \frac{Q_i(X)}{Q_i(x_i)}.$$

Hermite interpolation

Hermite interpolation is an application of the Chinese remainder theorem for univariate polynomials, which may involve moduli of arbitrary degrees (Lagrange interpolation involves only moduli of degree one).

The problem consists of finding a polynomial of the least possible degree, such that the polynomial and its first derivatives take given values at some fixed points.

More precisely, let $x_1, \ldots, x_k$ be k elements of the ground field K, and, for $i = 1, \ldots, k$, let $a_{i,0}, a_{i,1}, \ldots, a_{i,r_i-1}$ be the values of the first r_i derivatives of the sought polynomial at x_i (including the 0th derivative, which is the value of the polynomial itself). The problem is to find a polynomial $P(X)$ such that its jth derivative takes the value $a_{i,j}$ at x_i, for $i = 1, \ldots, k$ and $j = 0, \ldots, r_j$.

Consider the polynomial

$$P_i(X) = \sum_{j=0}^{r_i-1} \frac{a_{i,j}}{j!}(X - x_i)^j.$$

This is the Taylor polynomial of order $r_i - 1$ at x_i, of the unknown polynomial $P(X)$. Therefore, we must have

$$P(X) \equiv P_i(X) \pmod{(X - x_i)^{r_i}}.$$

Conversely, any polynomial $P(X)$ that satisfies these k congruences, in particular verifies, for any $i = 1, \ldots, k$

$$P(X) = P_i(X) + o(X - x_i)^{r_i-1}$$

therefore $P_i(X)$ is its Taylor polynomial of order $r_i - 1$ at x_i, that is, $P(X)$ solves the initial Hermite interpolation problem. The Chinese remainder theorem asserts that there exists exactly one polynomial of degree less than the sum of the r_i, which satisfies these k congruences.

There are several ways for computing the solution $P(X)$. One may use the method described at the beginning of § Over univariate polynomial rings and Euclidean domains. One may also use the constructions given in § Existence (constructive proof) or § Existence (direct proof).

Generalization to non-coprime moduli

The Chinese remainder theorem can be generalized to non-coprime moduli. Let m, n, a, b be any integers,

let $g = \gcd(m, n)$; $M = \operatorname{lcm}(m, n)$, and consider the system of congruences:

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}, \end{aligned}$$

If $a \equiv b \pmod{g}$, then this system has a unique solution modulo $M = mn/g$. Otherwise, it has no solutions.

If one uses Bézout's identity to write $g = um + vn$, then the solution is given by

$$x = \frac{avn + bum}{g}.$$

This defines an integer, as g divides both m and n. Otherwise, the proof is very similar to that for coprime moduli.[16]

Generalization to arbitrary rings

The Chinese remainder theorem can be generalized to any ring, by using coprime ideals (also called comaximal ideals). Two ideals I and J are coprime if there are elements $i \in I$ and $j \in J$ such that $i + j = 1$. This relation plays the role of Bézout's identity in the proofs related to this generalization, which otherwise are very similar. The generalization may be stated as follows.[17][18]

Let I_1, ..., I_k be two-sided ideals of a ring R and let I be their intersection. If the ideals are pairwise coprime, we have the isomorphism:

$$\begin{aligned} R/I &\to (R/I_1) \times \cdots \times (R/I_k) \\ x \bmod I &\mapsto (x \bmod I_1, \ldots, x \bmod I_k), \end{aligned}$$

between the quotient ring R/I and the direct product of the R/I_i, where "$x \bmod I$" denotes the image of the element x in the quotient ring defined by the ideal I. Moreover, if R is commutative, then the ideal intersection of pairwise coprime ideals is equal to their product; that is

$$I = I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k,$$

if I_i and I_j are coprime for all $i \neq j$.

Interpretation in terms of idempotents

Let $I_1, I_2, \ldots, I_k$ be pairwise coprime two-sided ideals with $\bigcap_{i=1}^{k} I_i = 0$, and

$$\varphi : R \to (R/I_1) \times \cdots \times (R/I_k)$$

be the isomorphism defined above. Let $f_i = (0, \ldots, 1, \ldots, 0)$ be the element of $(R/I_1) \times \cdots \times (R/I_k)$ whose components are all 0 except the ith which is 1, and $e_i = \varphi^{-1}(f_i)$.

The e_i are central idempotents that are pairwise orthogonal; this means, in particular, that $e_i^2 = e_i$ and $e_i e_j = e_j e_i = 0$ for every i and j. Moreover, one has $e_1 + \cdots + e_n = 1$, and $I_i = R(1 - e_i)$.

In summary, this generalized Chinese remainder theorem is the equivalence between giving pairwise coprime two-sided ideals with a zero intersection, and giving central and pairwise orthogonal idempotents that sum to 1.[19]

Applications

Sequence numbering

The Chinese remainder theorem has been used to construct a Gödel numbering for sequences, which is involved in the proof of Gödel's incompleteness theorems.

Fast Fourier transform

The prime-factor FFT algorithm (also called Good-Thomas algorithm) uses the Chinese remainder theorem for reducing the computation of a fast Fourier transform of size $n_1 n_2$ to the computation of two fast Fourier transforms of smaller sizes n_1 and n_2 (providing that n_1 and n_2 are coprime).

Encryption

Most implementations of RSA use the Chinese remainder theorem during signing of HTTPS certificates and during decryption.

The Chinese remainder theorem can also be used in secret sharing, which consists of distributing a set of shares among a group of people who, all together (but no one alone), can recover a certain secret from the given set of shares. Each of the shares is represented in a congruence, and the solution of the system of congruences using the Chinese remainder theorem is the secret to be recovered. Secret sharing using the Chinese remainder theorem uses, along with the Chinese remainder theorem, special sequences of integers that guarantee the impossibility of recovering the secret from a set of shares with less than a certain cardinality.

Range ambiguity resolution

The range ambiguity resolution techniques used with medium pulse repetition frequency radar can be seen as a special case of the Chinese remainder theorem.

Decomposition of surjections of finite abelian groups

Given a surjection $\mathbb{Z}/n \to \mathbb{Z}/m$ of finite abelian groups, we can use the Chinese remainder theorem to give a complete description of any such map. First of all, the theorem gives isomorphisms

$$\mathbb{Z}/n \cong \mathbb{Z}/p_{n_1}^{a_1} \times \cdots \times \mathbb{Z}/p_{n_i}^{a_i}$$
$$\mathbb{Z}/m \cong \mathbb{Z}/p_{m_1}^{b_1} \times \cdots \times \mathbb{Z}/p_{m_j}^{b_j}$$

where $\{p_{m_1}, \ldots, p_{m_j}\} \subseteq \{p_{n_1}, \ldots, p_{n_i}\}$. In addition, for any induced map

$$\mathbb{Z}/p_{n_k}^{a_k} \to \mathbb{Z}/p_{m_l}^{b_l}$$

from the original surjection, we have $a_k \geq b_l$ and $p_{n_k} = p_{m_l}$, since for a pair of primes p, q, the only non-zero surjections

$$\mathbb{Z}/p^a \to \mathbb{Z}/q^b$$

can be defined if $p = q$ and $a \geq b$.

These observations are pivotal for constructing the ring of profinite integers, which is given as an inverse limit of all such maps.

Dedekind's theorem

Dedekind's theorem on the linear independence of characters. Let M be a monoid and k an integral domain, viewed as a monoid by considering the multiplication on k. Then any finite family $(f_i)_{i\in I}$ of distinct monoid homomorphisms $f_i : M \to k$ is linearly independent. In other words, every family $(\alpha_i)_{i\in I}$ of elements $\alpha_i \in k$ satisfying

$$\sum_{i\in I} \alpha_i f_i = 0$$

must be equal to the family $(0)_{i\in I}$.

Proof. First assume that k is a field, otherwise, replace the integral domain k by its quotient field, and nothing will change. We can linearly extend the monoid homomorphisms $f_i : M \to k$ to k-algebra homomorphisms $F_i : k[M] \to k$, where $k[M]$ is the monoid ring of M over k. Then, by linearity, the condition

$$\sum_{i\in I} \alpha_i f_i = 0,$$

yields

$$\sum_{i\in I} \alpha_i F_i = 0.$$

Next, for $i, j \in I$; $i \neq j$ the two k-linear maps $F_i : k[M] \to k$ and $F_j : k[M] \to k$ are not proportional to each other. Otherwise f_i and f_j would also be proportional, and thus equal since as monoid homomorphisms they satisfy: $f_i(1) = 1 = f_j(1)$, which contradicts the assumption that they are distinct.

Therefore, the kernels $\operatorname{Ker} F_i$ and $\operatorname{Ker} F_j$ are distinct. Since $k[M]/\operatorname{Ker} F_i \cong F_i(k[M]) = k$ is a field, $\operatorname{Ker} F_i$ is a maximal ideal of $k[M]$ for every i in I. Because they are distinct and maximal the ideals $\operatorname{Ker} F_i$ and $\operatorname{Ker} F_j$ are coprime whenever $i \neq j$. The Chinese Remainder Theorem (for general rings) yields an isomorphism:

$$\phi : k[M]/K \to \prod_{i\in I} k[M]/\operatorname{Ker} F_i$$
$$\phi(x + K) = (x + \operatorname{Ker} F_i)_{i\in I}$$

where

$$K = \prod_{i \in I} \mathbf{Ker} F_i = \bigcap_{i \in I} \mathbf{Ker} F_i.$$

Consequently, the map

$$\begin{aligned} \Phi : k[M] &\to \prod_{i \in I} k[M]/\mathbf{Ker} F_i \\ \Phi(x) &= (x + \mathbf{Ker} F_i)_{i \in I} \end{aligned}$$

is surjective. Under the isomorphisms $k[M]/\mathrm{Ker}\, F_i \to F_i(k[M]) = k$, the map Φ corresponds to:

$$\begin{aligned} \psi : k[M] &\to \prod_{i \in I} k \\ \psi(x) &= [F_i(x)]_{i \in I} \end{aligned}$$

Now,

$$\sum_{i \in I} \alpha_i F_i = 0$$

yields

$$\sum_{i \in I} \alpha_i u_i = 0$$

for every vector $(u_i)_{i \in I}$ in the image of the map ψ. Since ψ is surjective, this means that

$$\sum_{i \in I} \alpha_i u_i = 0$$

for every vector

$$(u_i)_{i \in I} \in \prod_{i \in I} k.$$

Consequently, $(\alpha_i)_{i \in I} = (0)_{i \in I}$. QED.

See also

- Covering system
- Hasse principle
- Residue number system

Notes

1. Katz 1998, p. 197
2. Dence & Dence 1999, p. 156
3. Dauben 2007, p. 302
4. Kak 1986

5. Pisano 2002, pp. 402–403
6. Dauben 2007, p. 310
7. Libbrecht 1973
8. Gauss 1986, Art. 32–36
9. Ireland & Rosen 1990, p. 36
10. Ore 1988, p. 247
11. Ore 1988, p. 245
12. Ireland & Rosen 1990, p. 34
13. Ireland & Rosen 1990, p. 35
14. Duchet 1995
15. Rosen 1993, p. 136
16. Ore 1952.
17. Ireland & Rosen 1990, p. 181
18. Sengupta 2012, p. 313
19. Bourbaki, N. 1989, p. 110

References

- Dauben, Joseph W. (2007), "Chapter 3: Chinese Mathematics", in Katz, Victor J. (ed.), *The Mathematics of Egypt, Mesopotamia, China, India and Islam : A Sourcebook*, Princeton University Press, pp. 187–384, ISBN 978-0-691-11485-9
- Dence, Joseph B.; Dence, Thomas P. (1999), *Elements of the Theory of Numbers* (https://books.google.com/books?id=YiYHw7evhjkC&pg=PA156), Academic Press, ISBN 9780122091308
- Duchet, Pierre (1995), "Hypergraphs", in Graham, R. L.; Grötschel, M.; Lovász, L. (eds.), *Handbook of combinatorics, Vol. 1, 2*, Amsterdam: Elsevier, pp. 381–432, MR 1373663 (https://mathscinet.ams.org/mathscinet-getitem?mr=1373663). See in particular Section 2.5, "Helly Property", pp. 393–394 (https://books.google.com/books?id=5Y9NCwlx63IC&pg=PA393).
- Gauss, Carl Friedrich (1986), *Disquisitiones Arithemeticae* (https://www.springer.com/mathematics/algebra/book/978-0-387-96254-2), translated by Clarke, Arthur A. (Second, corrected ed.), New York: Springer, ISBN 978-0-387-96254-2
- Ireland, Kenneth; Rosen, Michael (1990), *A Classical Introduction to Modern Number Theory* (2nd ed.), Springer-Verlag, ISBN 0-387-97329-X
- Kak, Subhash (1986), "Computational aspects of the Aryabhata algorithm" (http://www.ece.lsu.edu/kak/AryabhataAlgorithm.pdf) (PDF), *Indian Journal of History of Science*, **21** (1): 62–71
- Katz, Victor J. (1998), *A History of Mathematics / An Introduction* (https://archive.org/details/historyofmathema00katz) (2nd ed.), Addison Wesley Longman, ISBN 978-0-321-01618-8
- Libbrecht, Ulrich (1973), *Chinese Mathematics in the Thirteenth Century: the "Shu-shu Chiu-chang" of Ch'in Chiu-shao*, Dover Publications Inc, ISBN 978-0-486-44619-6
- Ore, Øystein (1952), "The general Chinese remainder theorem", *The American Mathematical Monthly*, **59** (6): 365–370, doi:10.2307/2306804 (https://doi.org/10.2307%2F2306804), JSTOR 2306804 (https://www.jstor.org/stable/2306804), MR 0048481 (https://mathscinet.ams.org/mathscinet-getitem?mr=0048481)
- Ore, Oystein (1988) [1948], *Number Theory and Its History* (https://archive.org/details/numbertheoryitsh0000orey), Dover, ISBN 978-0-486-65620-5
- Pisano, Leonardo (2002), *Fibonacci's Liber Abaci* (https://www.springer.com/mathematics/book/978-0-387-40737-1), translated by Sigler, Laurence E., Springer-Verlag, pp. 402–403, ISBN 0-387-95419-8
- Rosen, Kenneth H. (1993), *Elementary Number Theory and its Applications* (3rd ed.), Addison-Wesley,

ISBN 978-0201-57889-8
- Sengupta, Ambar N. (2012), *Representing Finite Groups, A Semisimple Introduction*, Springer, ISBN 978-1-4614-1232-8
- Bourbaki, N. (1989), *Algebra I* (https://books.google.com/books?id=STS9aZ6F204C&q=%22associative+algebra%22), Springer, ISBN 3-540-64243-9

Further reading

- Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2001), *Introduction to Algorithms* (Second ed.), MIT Press and McGraw-Hill, ISBN 0-262-03293-7. See Section 31.5: The Chinese remainder theorem, pp. 873–876.
- Ding, Cunsheng; Pei, Dingyi; Salomaa, Arto (1996), *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography* (https://archive.org/details/chineseremainder0000ding/page/1), World Scientific Publishing, pp. 1–213 (https://archive.org/details/chineseremainder0000ding/page/1), ISBN 981-02-2827-9
- Hungerford, Thomas W. (1974), *Algebra* (https://www.springer.com/mathematics/algebra/book/978-0-387-90518-1), Graduate Texts in Mathematics, Vol. 73, Springer-Verlag, pp. 131–132, ISBN 978-1-4612-6101-8
- Knuth, Donald (1997), *The Art of Computer Programming*, vol. 2: *Seminumerical Algorithms* (Third ed.), Addison-Wesley, ISBN 0-201-89684-2. See Section 4.3.2 (pp. 286–291), exercise 4.6.2–3 (page 456).

External links

- "Chinese remainder theorem" (https://www.encyclopediaofmath.org/index.php?title=Chinese_remainder_theorem), *Encyclopedia of Mathematics*, EMS Press, 2001 [1994]
- Weisstein, Eric W., "Chinese Remainder Theorem" (https://mathworld.wolfram.com/ChineseRemainderTheorem.html), *MathWorld*
- Chinese Remainder Theorem (https://planetmath.org/ChineseRemainderTheorem) at PlanetMath.
- Full text of the Sun-tzu Suan-ching (http://ctext.org/sunzi-suan-jing) (Chinese) – Chinese Text Project
- Chinese remainder theorem at ProofWiki