

Chinese Remainder Theorem - GeeksforGeeks

Source: <https://www.geeksforgeeks.org/chinese-remainder-theorem/>

Courses Tutorials Practice Jobs Number System and Arithmetic Algebra Set Theory Probability Statistics Geometry Calculus Logarithms Mensuration Matrices Trigonometry Mathematics Technical Scriptor 2026 Explore Basic Arithmetic Numbers in Maths Arithmetic Operations Fractions in Maths Decimals in Maths Exponents Percentage Algebra Variable in Maths Polynomials Coefficient Algebraic Identities Properties of Algebraic Operations Geometry Lines and Angles Geometric Shapes in Maths Area and Perimeter of Shapes | Formula and Examples Surface Areas and Volumes Points, Lines and Planes Coordinate Axes and Coordinate Planes in 3D space Trigonometry & Vector Algebra Trigonometric Ratios Trigonometric Equations | Definition, Examples & How to Solve Trigonometric Identities Trigonometric Functions Inverse Trigonometric Functions Inverse Trigonometric Identities Calculus Introduction to Differential Calculus Limits in Calculus Continuity of Functions Differentiation Differentiability of Functions Integration Probability and Statistics Basic Concepts of Probability Bayes' Theorem Probability Distribution - Function, Formula, Table Descriptive Statistic What is Inferential Statistics? Measures of Central Tendency in Statistics Set Theory Practice NCERT Solutions for Class 8 to 12 RD Sharma Class 8 Solutions for Maths: Chapter Wise PDF RD Sharma Class 9 Solutions RD Sharma Class 10 Solutions RD Sharma Class 11 Solutions for Maths RD Sharma Class 12 Solutions for Maths Three 90 Challenge 90% Refund Chinese Remainder Theorem Last Updated : 5 Dec, 2025

Chinese Remainder Theorem is a mathematical principle that solves systems of modular equations by finding a unique solution from the remainder of the division. It is used in cryptography and computer science for efficient computation. According to the Theorem, if in a given set of equations, each equation has a different number (say, n_1, n_2, \dots, n_k), and these numbers are all relatively prime to each other, and also have some numbers (say, a_1, a_2, \dots, a_k), then there is a unique solution (let's call it x) that satisfies all the equations at once. This solution is found modulo the product of all the numbers ($N = n_1 \cdot n_2 \cdot \dots \cdot n_k$). Therefore, x satisfies each equation by leaving the same remainder when divided by its corresponding number (n_i) as the given number (a_i). In simpler terms, the theorem states: "If a number is divided by several other numbers that have no common factors, one can find the remainder when dividing by the product of those numbers." The solution is unique modulo N , meaning any other solution is congruent to the original one modulo N .

Statement of Chinese Remainder Theorem The Chinese Remainder Theorem states that a system of simultaneous congruences, defined by pairwise coprime positive integers (n_1, n_2, \dots, n_k) and arbitrary integers (a_1, a_2, \dots, a_k) such as: $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, ..., $x \equiv a_k \pmod{n_k}$ there exists a unique solution x modulo ($N = n_1 \cdot n_2 \cdot \dots \cdot n_k$) that satisfies all the congruences simultaneously.

Chinese Remainder Theorem Proof To prove Chinese remainder theorem, let us find an integer (x) that satisfies: $x \equiv a_i \pmod{n_i}$ for each ($i = 1, 2, \dots, k$). We define ($N_i = N/n_i$). Since (n_i) and (N_i) are coprime, according to Bézout's identity, there are integers (s_i) and (t_i) such that: $s_i \cdot n_i + t_i \cdot N_i = 1$. We set ($y_i = t_i \cdot N_i$). Now, let's construct (x) as follows, $x = \sum_{i=1}^k a_i \cdot y_i$. This solution satisfies all the congruences, i.e., $x \equiv a_i \pmod{n_i}$ for each (i). To see this, observe: $x \equiv a_i \cdot y_i \equiv a_i \cdot t_i \cdot N_i \equiv a_i \cdot 1 \equiv a_i$. Thus, (x) is a solution to the system of congruences.

Uniqueness : Suppose (x) and (x') are two solutions to the system of congruences. We aim to show that ($x \equiv x' \pmod{N}$). Let ($m = x' - x$). Since both (x) and (x') satisfy all the congruences, (m) must also satisfy them. Therefore, (m) is divisible by each of the moduli (n_1, n_2, \dots, n_k). By definition, ($N = n_1 \cdot n_2 \cdot \dots \cdot n_k$). As (m) is divisible by each (n_i), it is also divisible by (N), i.e., $m \equiv 0 \pmod{N}$. Hence, $x \equiv x' \pmod{N}$, establishing uniqueness).

Necessary Condition for Chinese Remainder Theorem For the Chinese Remainder Theorem to work, the numbers we are dividing by must not have any common factors. So, if there are two numbers that are being divided by, say (m_i) and (m_j), then they can not common factors other than 1. That means their biggest shared factor, called the greatest common divisor is 1. $\text{GCD}(m_i, m_j) = 1$. This condition ensures that the system of congruences is consistent and that the solution provided by the Chinese Remainder Theorem is unique modulo the product of the moduli. If the moduli are not pairwise coprime, then the theorem may not yield a solution, or the solution may not be unique. Therefore, pairwise coprimality is a fundamental requirement for the application of the Chinese Remainder Theorem.

Chinese Remainder Theorem Solution for Two Moduli Chinese Remainder Theorem provides a solution for systems of congruences involving two moduli. Given two pairwise coprime moduli (m_1)

and (m_2) , and their respective residues (a_1) and (a_2) , the theorem states that there exists a unique solution modulo $(m_1 \times m_2)$ for the system of congruences: $x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$. The solution can be found using the formula: $x = a_1 + m_1 \left(\frac{a_2 - a_1}{m_2} \right) \left(\frac{m_1^{-1} \pmod{m_2}}{m_2} \right) \pmod{m_1 \times m_2}$. Where $(m_1^{-1} \pmod{m_2})$ denotes the modular multiplicative inverse of (m_1) modulo (m_2) . This inverse can be found using methods such as the Extended Euclidean Algorithm.

Extended Euclidean Algorithm : Computes the gcd of two integers a and b , along with integers x and y (called Bézout coefficients) such that: $a \cdot x + b \cdot y = \gcd(a, b)$. where, Two integers a and b ($a > b$). $\gcd(a, b)$: Greatest common divisor. x, y : Integers satisfying $a \cdot x + b \cdot y = \gcd(a, b)$. It is widely used to find modular inverses (critical in cryptography).

Chinese Remainder Theorem Solution for General Case Chinese Remainder Theorem (CRT) provides a solution for a system of congruences with arbitrary moduli. Suppose we have a system of congruences: $x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$ \dots $x \equiv a_n \pmod{m_n}$ Where (m_1, m_2, \dots, m_n) are pairwise coprime moduli and (a_1, a_2, \dots, a_n) are the corresponding residues. CRT states that there exists a unique solution modulo $(M = m_1 \times m_2 \times \dots \times m_n)$ for this system of congruences. The solution can be found using the formula: $x \equiv \sum_{i=1}^n a_i M_i y_i \pmod{M}$ Where $(M_i = M / m_i)$ and (y_i) is the modular multiplicative inverse of (M_i) modulo (m_i) . Suppose we have the following system of congruences: $x \equiv 2 \pmod{3}$ $x \equiv 3 \pmod{5}$ $x \equiv 2 \pmod{7}$. Calculate $M = 3 \times 5 \times 7 = 105$. Then, we calculate $(M_1 = 105 / 3 = 35)$, $(M_2 = 105 / 5 = 21)$, and $(M_3 = 105 / 7 = 15)$. find the modular multiplicative inverses (y_1) , (y_2) , and (y_3) for (M_1) , (M_2) , and (M_3) modulo (m_1) , (m_2) , and (m_3) , respectively. y_1 is the modular multiplicative inverse of 35 modulo 3, which is 2. y_2 is the modular multiplicative inverse of 21 modulo 5, which is 1. y_3 is the modular multiplicative inverse of 15 modulo 7, which is 1. Now, using the formula: $x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{105}$ $x \equiv 140 + 63 + 30 \pmod{105}$ $x \equiv 233 \pmod{105}$. So, the solution for the system of congruences is $x \equiv 233 \pmod{105}$.

Chinese Remainder Theorem Solution for Not Coprime Moduli Chinese Remainder Theorem helps in solving systems of equations where the remainders are congruent, even if the numbers that are divisible by are not relatively prime. But when the divisors are not relatively prime, there might be more than one solution to the problem. Suppose we have the following system of congruences: $x \equiv 2 \pmod{4}$ $x \equiv 6 \pmod{6}$. Here, the moduli 4 and 6 are not coprime because their greatest common divisor (GCD) is 2. To find the solution using the Chinese Remainder Theorem, we proceed as follows: 1. Find the moduli product: Calculate $(m = 4 \times 6 = 24)$. 2. Find the residues: Divide each modulus by the product of the other moduli to find the residue: $4 \times k \equiv 1 \pmod{6}$ $6 \times k' \equiv 1 \pmod{4}$. In this case, $(k = 1)$ and $(k' = 1)$ satisfy the congruences, so the residues are both 1. 3. Calculate the solution: The solution (x) is given by: $x = a_1 \times m_2 \times k + a_2 \times m_1 \times k' \pmod{m}$. Plugging in the values: $x = 2 \times 6 \times 1 + 6 \times 4 \times 1 \pmod{24}$ $x = 12 + 24 \pmod{24}$ $x = 36 \pmod{24}$ $x = 12$. So, the solution for this system of congruences is $x \equiv 12 \pmod{24}$. Also Check: Chinese Remainder Theorem in Program (DSA) Chinese Remainder Theorem in Python Implementation of CRT Application of Chinese Remainder Theorem in Computer Science Applications of the Chinese remainder theorem are as follows: Cryptography RSA Decryption is optimized using CRT. RSA decryption computes $m \equiv c \cdot d \pmod{N}$, where $N = p \cdot q$ (large primes). Direct computation is slow for large N and CRT does the process of direct exponentiation $\sim 4\times$ faster. CRT enables parallel processing of encrypted data by splitting computations across smaller residues. Used in secure multi-party computation (MPC) and private AI training. Error correction Reed-Solomon Codes recover data from corrupted storage (e.g., CDs, QR codes) by encoding data as residues modulo coprime numbers. Even if some residues are lost/corrupted, original data can be reconstructed. Ex.: RAID storage systems, satellite communications. Checksum Algorithms CRT-based checksums detect errors in distributed databases. Parallel Computing Residue Number Systems (RNS), As large integer arithmetic is slow due to carry propagation. CRT represent numbers as residues modulo small primes and perform carry-free parallel arithmetic (addition, multiplication). GPU Acceleration, CRT decomposes problems into independent sub-tasks, ideal for massively parallel GPU computing. Quantum Computing For Quantum Error Correction, CRT helps design fault-tolerant quantum gates by decomposing operations into smaller moduli. In Shor's Algorithm, CRT is used in the final step to reconstruct the prime factors of large integers. Algorithmic Optimizations For Fast Fourier Transform (FFT), CRT enables multidimensional FFTs by breaking signals into smaller residues. In Knuth's Modular Multiplication, CRT speeds up large-integer multiplication in cryptographic libraries.

Solved Example on Chinese Remainder Theorem Suppose a certain number leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7. Find the smallest positive integer that satisfies these conditions using the Chinese Remainder Theorem.

Solution: Let x be the number that satisfies all the given conditions: Remainder of 2 when divided by 3
 Remainder of 3 when divided by 5 Remainder of 2 when divided by 7 Now, as per the Chinese
 Remainder Theorem, since the moduli (3, 5, and 7) are pairwise coprime, a unique solution modulo is
 $\text{lcm}(3,5,7)=105$ $x \equiv 2 \pmod{3}$ $x \equiv 3 \pmod{5}$ $x \equiv 2 \pmod{7}$ The modular inverses for each modulus will be:
 For 3, the modular inverse of 3 modulo 5 is 2 as $3 \cdot 2 \equiv 1 \pmod{5}$ For 5, the modular inverse of 5 modulo
 7 is 3 as $5 \cdot 3 \equiv 1 \pmod{7}$ For 7, the modular inverse of 7 modulo 3 is 1 as $7 \cdot 1 \equiv 1 \pmod{3}$ Now calculate
 for x : $x \equiv (2 \cdot 35 \cdot 2) + (3 \cdot 3 \cdot 7 \cdot 1) + (2 \cdot 3 \cdot 5) \cdot (1 \cdot 1) \pmod{105}$ On solving each term we get, $x \equiv 140 + 63$
 $+ 30 \pmod{105}$ $x \equiv 233 \pmod{105}$ $x \equiv 23 \pmod{105}$ \therefore Smallest positive integer that satisfies the given
 conditions is $x = 23$. Practice Questions on Chinese Remainder Theorem Question 1: Solve the system
 of congruences: $x \equiv 2 \pmod{3}$ $x \equiv 3 \pmod{5}$ $x \equiv 2 \pmod{7}$ Question 2: Solve the system of
 congruences: $x \equiv 1 \pmod{2}$ $x \equiv 2 \pmod{4}$ $x \equiv 3 \pmod{5}$ Answer Key $x = 23 \pmod{105}$. There is no
 solution for this system of congruences, because $x \equiv 1 \pmod{2}$ (odd) and $x \equiv 2 \pmod{4}$ (even) are
 contradictory. Comment Article Tags: Article Tags: Mathematics School Learning Algebra