Chinese remainder theorem

From Wikipedia, the free encyclopedia

Chinese remainder theorem refers to a result about congruences in number theory and its generalizations in abstract algebra.

Contents

Theorem statement

The original form of the theorem, contained in a third-century AD book by Chinese mathematician Sun Tzu [1] (http://www.economist.com/science/displaystory.cfm?story_id=8881479) and later republished in a 1247 book by Qin Jiushao, is a statement about simultaneous congruences (see modular arithmetic).

Suppose n_1, n_2, …, n_k are integers which are pairwise coprime. Then, for any given integers a_1,a_2, …, a_k, there exists an integer x solving the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Furthermore, all solutions x to this system are congruent modulo the product $N = n_1 n_2 \ldots n_k$.

Sometimes, the simultaneous congruences can be solved even if the n_i's are not pairwise coprime. A solution x exists if and only if:

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)} \qquad \text{for all } i \text{ and } j.$$

All solutions x are then congruent modulo the least common multiple of the n_i.

Versions of the Chinese remainder theorem were also known to Brahmagupta, and appear in Fibonacci's Liber Abaci (1202).

A constructive algorithm to find the solution

This algorithm only treats the situations where the n_i's are coprime. The method of successive substitution can often yield solutions to simultaneous congruences, even when the moduli are not pairwise coprime.

Suppose, as above, that a solution is needed to the system of congruences:

$$x \equiv a_i \pmod{n_i} \quad \text{for } i = 1, \ldots, k.$$

Again, to begin, the product $N = n_1 n_2 \ldots n_k$ is defined. Then a solution x can be found as follows.

For each i the integers n_i and N / n_i are coprime. Using the extended Euclidean algorithm we can therefore find integers r_i and s_i such that $r_i n_i + s_i N / n_i = 1$. Then, choosing the label $e_i = s_i N / n_i$, the above expression becomes:

$$r_i n_i + e_i = 1$$

Consider e_i. The above equation guarantees that its remainder, when divided by n_i, must be 1. On the other hand, since it is formed as $s_i N / n_i$, the presence of N guarantees that it's evenly divisible by any n_j so long as $j \neq i$.

$$e_i \equiv 1 \pmod{n_i} \quad \text{and} \quad e_i \equiv 0 \pmod{n_j} \quad \text{for } i \neq j$$

Because of this, combined with the multiplication rules allowed in congruences, one solution to the system of simultaneous congruences is:

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

For example, consider the problem of finding an integer x such that

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{4}, \\ x &\equiv 1 \pmod{5}. \end{aligned}$$

Using the extended Euclidean algorithm for 3 and 4×5 = 20, we find (−13) × 3 + 2 × 20 = 1, i.e. $e_1 = 40$. Using the Euclidean algorithm for 4 and 3×5 = 15, we get (−11) × 4 + 3 × 15 = 1. Hence, $e_2 = 45$. Finally, using the Euclidean algorithm for 5 and 3×4 = 12, we get 5 × 5 + (−2) × 12 = 1, meaning $e_3 = -24$. A solution x is therefore 2 × 40 + 3 × 45 + 1 × (−24) = 191. All other solutions are congruent to 191 modulo 60, (3 × 4 × 5 = 60) which means that they are all congruent to 11 modulo 60.

NOTE: There are multiple implementations of the extended Euclidean algorithm which will yield different sets of e_1, e_2, and e_3. These sets however will produce the same solution i.e. 11 modulo 60.

Statement for principal ideal domains

For a principal ideal domain R the Chinese remainder theorem takes the following form: If u_1, ..., u_k are elements of R which are pairwise coprime, and u denotes the product $u_1...u_k$, then the quotient ring R/uR and the product ring $R/u_1R \times \cdots \times R/u_kR$ are isomorphic via the isomorphism

$$f : R/uR \rightarrow R/u_1R \times \cdots \times R/u_kR$$

such that

$$f(x + uR) = (x + u_1R, \ldots, x + u_kR) \quad \text{for every } x \in R.$$

This isomorphism is unique; the inverse isomorphism can be constructed as follows. For each i, the elements u_i and u/u_i are coprime, and therefore there exist elements r and s in R with

$$ru_i + su/u_i = 1.$$

Set $e_i = s\, u/u_i$. Then the inverse of f is the map

$$g : R/u_1R \times \cdots \times R/u_kR \rightarrow R/uR$$

such that

$$g(a_1 + u_1R, \ldots, a_k + u_kR) = \left(\sum_{i=1}^{k} a_i e_i\right) + uR \quad \text{for all } a_1, \ldots, a_k \in R.$$

Note that this statement is a straightforward generalization of the above theorem about integer congruences: the ring **Z** of integers is a principal ideal domain, the surjectivity of the map f shows that every system of congruences of the form

$$x \equiv a_i \pmod{u_i} \quad \text{for } i = 1, \ldots, k$$

can be solved for x, and the injectivity of the map f shows that all the solutions x are congruent modulo u.

Statement for general rings

The general form of the Chinese remainder theorem, which implies all the statements given above, can be formulated for rings and (two-sided) ideals. If R is a ring and I_1, ..., I_k are two-sided ideals of R which are pairwise coprime (meaning that $I_i + I_j = R$ whenever $i \neq j$), then the product I of these ideals is equal to their intersection, and the quotient ring R/I is isomorphic to the product ring R/I_1 x R/I_2 x ... x R/I_k via the isomorphism

$$f : R/I \rightarrow R/I_1 \times \cdots \times R/I_k$$

such that

$$f(x+I) = (x+I_1, \ldots, x+I_k) \quad \text{for all } x \in R.$$

Applications

In the RSA algorithm calculations are made modulo n, where n is a product of two primes p and q. Common sizes for n are 1024, 2048 or 4096 bits, making calculations very time-consuming. Using Chinese remaindering these calculations can be transported from the ring $\mathbb{Z}_n$ to the ring $\mathbb{Z}_p \times \mathbb{Z}_q$. The sum of the bit sizes of p and q is the bit size of n, making p and q considerably smaller than n. This greatly speeds up calculations. Note that RSA algorithm implementations using Chinese remaindering are more susceptible to fault injection attacks.

See also

- Covering system
- Residue number system

External links

- Chinese remainder theorem (http://www.cut-the-knot.org/blue/chinese.shtml) at cut-the-knot

References

- Donald Knuth. *The Art of Computer Programming*, Volume 2: *Seminumerical Algorithms*, Third Edition. Addison-Wesley, 1997. ISBN 0-201-89684-2. Section 4.3.2 (pp.286–291), exercise 4.6.2–3 (page 456).
- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Section 31.5: The Chinese remainder theorem, pp.873–876.
- Sigler, Laurence E. (trans.) (2002). *Fibonacci's Liber Abaci*. Springer-Verlag, 402–403. ISBN 0-387-95419-8.

Categories: Modular arithmetic | Commutative algebra | Mathematical theorems

---