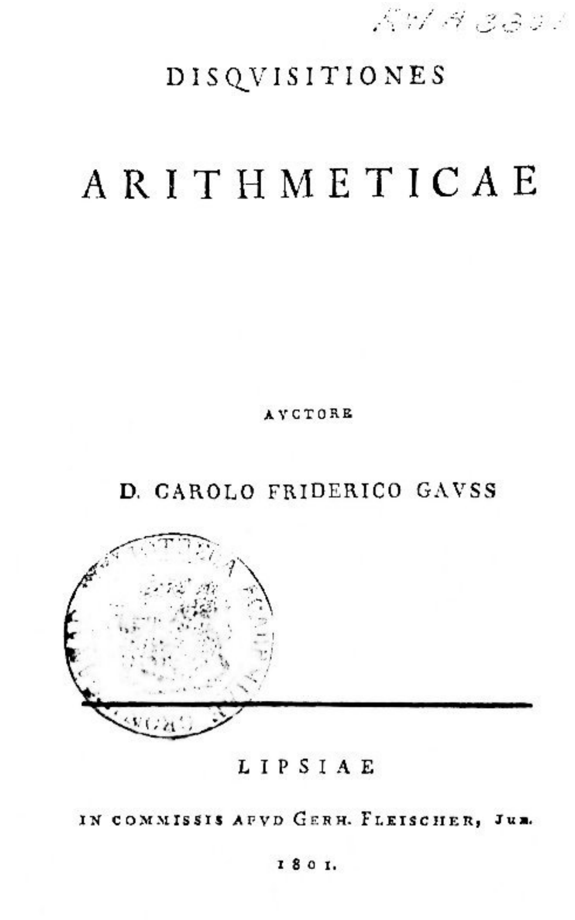
Chinese remainder theorem



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.[1]*

The **Chinese remainder theorem** is a result about congruences in number theory and its generalizations in abstract algebra. It was first published some time between the 3rd and 5th centuries by the Chinese mathematician Sun Tzu.

In its basic form, the Chinese remainder theorem will determine a number n that, when divided by some given divisors, leaves given remainders. In Sun Tzu's example (stated in modern terminology),*[2] what is the smallest number n that when divided by 3 leaves a remainder of 2, when divided by 5 leaves a remainder of 3, and when divided by 7 leaves a remainder of 2?

1 Theorem statement

Suppose n_1, ..., n_k are positive integers that are pairwise coprime. Then, for any given sequence of integers a_1, ..., a_k, there exists an integer x solving the following system of simultaneous congruences.

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

Furthermore, any two solutions of this system are congruent modulo the product, $N = n_1 \ldots n_k$.*[3] Hence, there is a unique (non-negative) solution less than N.

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

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)},$$

for all i and j. All solutions, x, are then congruent modulo the least common multiple of the n_i.*[4]

A modern restatement of the theorem in algebraic language is that for a positive integer with prime factorization

$$n = p_1^{r_1} \cdots p_k^{r_k},$$

we have the isomorphism between a ring and the direct sum of its prime power parts*[5]

$$\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/p_1^{r_1}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p_k^{r_k}\mathbf{Z}.$$

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.*[6]

2 Existence and uniqueness

Existence is established by an explicit construction of x.*[7] Let $[a^*{-}1]_b$ denote the multiplicative inverse of $a \pmod{b}$, that is, $a\,[a^*{-}1]_b \equiv 1 \pmod{b}$. It is defined exactly when a and b are coprime and can be obtained from the Extended Euclidean algorithm.

For notational convenience, with $N = n_1 n_2 ... n_k$, define N_j := N/n_j for j = 1, ..., k. Because the n_i's are relatively coprime, n_i divides N_j for each $i \neq j$ and we have

$$N_i \left[(N_i)^{-1}\right]_{n_i} \pmod{n_j} \equiv \delta_{ij},$$ (the Kronecker delta),

that is, 1 if $i = j$ and 0 if $i \neq j$. So, the expression

$$x := \sum_i a_i N_i \left[(N_i)^{-1}\right]_{n_i} = a_1 N_1 \left[(N_1)^{-1}\right]_{n_1} + a_2 N_2 \left[(N_2)^{-1}\right]_{n_2} + \cdots + a_k N_k \left[(N_k)^{-1}\right]_{n_k}$$

satisfies the congrugences $x \equiv a_i \pmod{n_i}$ for all i = 1, ..., k, since, for each i, all the terms on the right are zero except the i[*]th term, which evaluates to a_i.

Suppose that x and y are both solutions to all the congruences. Then $x - y \equiv 0 \pmod{n_i}$ for all i = 1, ..., k. Since the n_i are coprime, $x - y \equiv 0 \pmod{N}$. Therefore, any two solutions are congruent modulo N, or, stated another way, the solution is unique (mod N).

3 History

The earliest known statement of the theorem, as a problem with specific numbers, appears in the 3rd-century book *Sunzi's Mathematical Classic* (孫子算經) by the Chinese mathematician Sun Tzu.*[2] Sun Tzu's work contains neither a proof nor a full algorithm.*[8] What amounts to an algorithm for solving this problem was described by Aryabhata (6th century).*[9] Special cases of the Chinese remainder theorem were also known to Brahmagupta (7th century), and appear in Fibonacci's Liber Abaci (1202).*[10] The result was later generalized with a complete solution called *Dayanshu* (大衍術) in Qin Jiushao's 1247 *Mathematical Treatise in Nine Sections* (數書九章, *Shushu Jiuzhang*).*[11]

The notion of congruences was first introduced and used by Gauss in his *Disquisitiones Arithmeticae* of 1801.*[12] 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." *[13] Gauss introduces a procedure for solving the problem that had already been used by Euler but was in fact the ancient method that had appeared several times.*[14]

4 Finding the solution

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

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

4.1 Brute-force approach

A brute-force approach converts these congruences into sets and writes the elements out to the product of 3×4×5 = 60 (the solutions modulo 60 for each congruence):

x ∈ {2, 5, 8, **11**, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, **71**, 74, ...}

x ∈ {3, 7, **11**, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63, 67, **71**, 75, 79, ...}

x ∈ {1, 6, **11**, 16, 21, 26, 31, 36, 41, 46, 51, 56, 61, 66, **71**, 76, 81, 86, 91, 96, ...}

To find an x that satisfies all three congruences, intersect the three sets to get:

x ∈ {11, 71, ...}

Which can be expressed as

$$x \equiv 11 \pmod{60}$$

4.2 An algebraic approach

Another way to find a solution is with basic algebra, modular arithmetic, and stepwise substitution.

We start by translating these congruences into equations for some t, s, and u:

$$\begin{aligned} x &= 2 + 3t \\ x &= 3 + 4s \\ x &= 1 + 5u \end{aligned}$$

Start by substituting the x from the first equation into the second congruence:

$$\begin{aligned} 2 + 3t &\equiv 3 && \pmod{4} \\ 3t &\equiv 1 && \pmod{4} \\ t &\equiv (3)^{-1} \equiv 3 && \pmod{4} \end{aligned}$$

meaning that $t = 3 + 4s$ for some integer s. Substitute t into the first equation:

$$x = 2 + 3t = 2 + 3(3 + 4s) = 11 + 12s$$

Substitute this x into the third congruence:

$$\begin{aligned} 11 + 12s &\equiv 1 \pmod 5 \\ 1 + 2s &\equiv 1 \pmod 5 \\ 2s &\equiv 0 \pmod 5 \end{aligned}$$

meaning that $s = 0 + 5u$ for some integer u. Finally,

$$x = 11 + 12s = 11 + 12(5u) = 11 + 60u$$

So, we have solutions {11, 71, 131, 191, ...}.

Notice that 60 = lcm(3,4,5). If the moduli are pairwise coprime (as they are in this example), the solutions will be congruent modulo their product.

4.3 Using the existence construction

Since the n_i are pairwise coprime we may use the construction given in the existence section above. (For simultaneous congruences when the moduli are not pairwise coprime, one of the other methods given above can often yield solutions.)

In this example, $N = 3 \times 4 \times 5 = 60$, so $N_3 = N/3 = 20$, $N_4 = 15$ and $N_5 = 12$. Using the extended Euclidean algorithm, we obtain $[(N_3)^{*}{-1}]_3 \equiv 2$ (notice that 20 × 2 = 40 ≡ 1 (mod 3)), $[(N_4)^{*}{-1}]_4 \equiv 3$ and $[(N_5)^{*}{-1}]_5 \equiv 3$. Therefore, $x = 2(20)(2) + 3(15)(3) + 1(12)(3) = 80 + 135 + 36 = 251$. Since all solutions are congruent modulo N, the smallest non-negative solution is 11 ≡ 251 (mod 60).

Using the same principle, the answer to Sun Tzu's original question (in the introduction) is therefore **23**, since for divisors 3, 5, 7: 2(35)(2) + 3(21)(1) + 2(15)(1) = 233 ≡ 23 (mod 105).

5 Statement for principal ideal domains

Chinese Remainder Theorem for Principal Ideal Domains. Let R be principal ideal domain. If u_1, ..., u_k are pairwise coprime elements of R where $u = u_1...u_k$, then the quotient ring R/uR and the product ring $R/u_1R \times ... \times R/u_kR$ are isomorphic via the following map:

$$\begin{aligned} &f : R/uR \to R/u_1R \times \cdots \times R/u_kR \\ &f(x + uR) = (x + u_1R, \ldots, x + u_kR) \end{aligned}$$

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

$$x \equiv a_i \pmod{u_i} \qquad 1 \le i \le k$$

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

Proof. This map is well-defined and a homomorphism of rings. An inverse homomorphism can be constructed as follows, showing that it is in fact an isomorphism. 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 $e_i = su/u_i$. Then it is clear that

$$e_i \equiv \delta_{ij} \pmod{u_jR}.$$

Thus the inverse of f is the map

$$\begin{aligned} &g : R/u_1R \times \cdots \times R/u_kR \to R/uR \\ &g(a_1 + u_1R, \ldots, a_k + u_kR) = \sum_{i=1}^{k} a_ie_i + uR \end{aligned}$$

6 Statement for general rings

The general form of the Chinese remainder theorem, which implies all the statements given above, can be formulated for commutative rings and ideals.

Chinese Remainder Theorem for Commutative Rings. If R is a commutative ring with identity and I_1, ..., I_k are ideals of R that are pairwise coprime (meaning $I_i + I_j = R$ for all $i \neq j$), then the product I of these ideals is equal to their intersection, and the quotient ring R/I is isomorphic to the direct sum of rings $R/I_1 \oplus ... \oplus R/I_k$ via the isomorphism*[15]

$$\begin{aligned} &f\colon R/I \to R/I_1 \oplus \cdots \oplus R/I_k \\ &f(x + I) = (x + I_1, \cdots, x + I_k). \end{aligned}$$

Here is a version of the theorem where R is not required to be commutative:

Chinese Remainder Theorem for Noncommutative Rings. Let R be any ring with 1 (not necessarily commutative) and I_1, ..., I_k be pairwise coprime 2-sided ideals. Then the canonical ring homomorphism $R \to R/I_1 \times ... \times R/I_k$ is onto, with kernel $I_1 \cap ... \cap I_k$. Hence, $R/(I_1 \cap \cdots \cap I_k) \simeq R/I_1 \times \cdots \times R/I_k$.

7 Applications

7.1 Sequence numbering

The Chinese remainder theorem can be used to construct an elegant Gödel numbering for sequences, which is needed to prove Gödel's incompleteness theorems.

7.2 Fast Fourier transform

The Good-Thomas fast Fourier transform algorithm exploits a re-indexing of the data based on the Chinese remainder theorem. The Prime-factor FFT algorithm contains an implementation.

7.3 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.

7.4 Range ambiguity resolution

Main article: 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.

7.5 Hermite interpolation

The General Hermite Interpolation Problem. Given r complex points (“interpolation nodes”) $\lambda_1, \cdots, \lambda_r$ and complex data $\{a_{j,k}\colon 1 \le j \le r,\ 0 \le k < \nu_j\}$, find $P(x) \in \mathbf{C}[x]$ such that:

$$P^{(k)}(\lambda_j) = a_{j,k} \qquad 1 \le j \le r, \quad 0 \le k < \nu_j.$$

Solution. Introducing the polynomials

$$A_j(x) := \sum_{k=0}^{\nu_j - 1} \frac{a_{j,k}}{k!}(x-\lambda_j)^k$$

the problem may be equivalently reformulated as a system of r simultaneous congruences:

$$P(x) \equiv A_j(x) \pmod{(x-\lambda_j)^{\nu_j}}, \qquad 1 \le j \le r$$

By the Chinese remainder theorem in the principal ideal domain $\mathbf{C}[x]$, there is a unique polynomial $P(x)$ such that:

$$\deg(P) < n := \sum_j \nu_j.$$

A direct construction, in analogy with the above proof for the integer number case, can be performed as follows. Define the polynomials

$$Q = \prod_{i=1}^{r} (x-\lambda_i)^{\nu_i}$$
$$Q_j = \frac{Q}{(x-\lambda_j)^{\nu_j}}$$

The partial fraction decomposition of $1/Q$ gives r polynomials S_j with degrees $\deg(S_j) < \nu_j$ such that

$$\frac{1}{Q} = \sum_{i=1}^{r} \frac{S_i}{(x-\lambda_i)^{\nu_i}}$$

so that

$$1 = \sum_{i=1}^{r} S_i Q_i.$$

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

$$\sum_{i=1}^{r} A_i S_i Q_i = A_j + \sum_{i=1}^{r} (A_i - A_j) S_i Q_i \equiv A_j \pmod{(x-\lambda_j)^{\nu_j}} \qquad 1 \le$$

and the minimal degree solution is this one reduced modulo Q, that is the unique with degree less than n.

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

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

where

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

Consequently, the map

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

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

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

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.

8 Non-commutative case: a caveat

Sometimes in the commutative case, the conclusion of the Chinese Remainder Theorem is stated as $R/(I_1 \dots I_k) \cong R/I_1 \times \dots \times R/I_k$. This version does not hold in the non-commutative case, since $I_1 \cap \dots \cap I_k \neq I_1 \dots I_k$, as can be seen from the following case:

> **Proposition.** Let R be the ring of non-commutative real polynomials in x and y. Let I be the principal two-sided ideal generated by x and J the principal two-sided ideal generated by $xy + 1$. Then $I + J = R$ but $I \cap J \neq IJ$.

Proof. Observe that I is formed by all polynomials with an x in every term and that every polynomial in J vanishes under the substitution $y = -1/x$. Then clearly $p = (xy + 1)x \in I \cap J$. Define a “term in R”, as an element of the multiplicative monoid of R generated by x and y, and its degree as the usual degree of the term after the substitution $y = x$. On the other hand, suppose $q \in J$. Observe that a term in q of maximum degree depends on y otherwise q under the substitution $y = -1/x$ can not vanish. The same happens then for an element $q \in IJ$. Note that the last y, from left to right, in a term of maximum degree in an element of IJ is preceded by more than one x. (We are counting here all the preceding xs. E.g., in x^2yxyx^5 the last y is preceded by three xs.) This proves that $p = (xy + 1)x \notin IJ$ since the last y in the term of maximum degree in p (xyx) is preceded by only one x. Hence $I \cap J \neq IJ$.

However, it is true in general that $I + J = R$ implies $I \cap J = IJ + JI$. To see this, note that $I \cap J = (I \cap J)(I + J) \subset IJ + JI$, while the opposite inclusion is obvious. Also, we have in general that, provided $I_1, ..., I_m$ are pairwise coprime two-sided ideals in R, the natural map

$$R/(I_1 \cap \cdots \cap I_m) \to R/I_1 \oplus \cdots \oplus R/I_m$$

is an isomorphism. Note that $I_1 \cap ... \cap I_m$ can be replaced by a sum over all orderings of $I_1, ..., I_m$ of their product (or just a sum over enough orderings, using inductively that $I \cap J = IJ + JI$ for coprime ideals $I, J \subset R$).

9 See also

- Covering system
- Hasse principle
- Residue number system
- Secret sharing using the Chinese remainder theorem

10 Notes

[1] Gauss & Clarke 1986, Art. 32-36

[2] Katz 1998, p. 197

[3] Ireland & Rosen 1990, p. 34

[4] Ore 1988, p. 244

[5] Ireland & Rosen 1990, p. 35

[6] Duchet 1995

[7] Rosen 1993, p. 136

[8] Dauben 2007, p. 302

[9] Kak 1986

[10] Leonardo Pisano; Sigler, Laurence E. (translator into English) (2002), *Fibonacci's Liber Abaci*, Springer-Verlag, pp. 402–403, ISBN 0-387-95419-8

[11] Dauben 2007, p. 310

[12] Ireland & Rosen 1990, p. 36

[13] Ore 1988, p. 247

[14] Ore 1988, p. 245

[15] Ireland & Rosen 1990, p. 181

11 References

- Dauben, Joseph W. (2007), "Chapter 3: Chinese Mathematics", in Katz, Victor J., *The Mathematics of Egypt, Mesopotamia, China, India and Islam : A Sourcebook*, Princeton University Press, pp. 187–384, ISBN 978-0-691-11485-9
- Duchet, Pierre (1995), "Hypergraphs", in Graham, R. L.; Grötschel, M.; Lovász, L., *Handbook of combinatorics, Vol. 1, 2*, Amsterdam: Elsevier, pp. 381–432, MR 1373663. See in particular Section 2.5, "Helly Property", pp. 393–394.
- Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithemeticae* (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" (PDF), *Indian Journal of History of Science* **21** (1): 62–71
- Katz, Victor J. (1998), *A History of Mathematics / An Introduction* (2nd ed.), Addison Wesley Longman, ISBN 978-0-321-01618-8
- Ore, Oystein (1988) [1948], *Number Theory and Its History*, Dover, ISBN 978-0-486-65620-5
- Rosen, Kenneth H. (1993), *Elementary Number Theory and its Applications* (3rd ed.), Addison-Wesley, ISBN 978-0201-57889-8

12 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*, World Scientific Publishing, pp. 1–213, ISBN 981-02-2827-9
- Hungerford, Thomas W. (1974), *Algebra*, 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*, Volume 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).

13 External links

- Hazewinkel, Michiel, ed. (2001), “Chinese remainder theorem” , *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Weisstein, Eric W., “Chinese Remainder Theorem” , *MathWorld*.
- Full text of the Sunzi Suanjing (Chinese) —Chinese Text Project

14 Text and image sources, contributors, and licenses

14.1 Text

- **Chinese remainder theorem** *Source:* https://en.wikipedia.org/wiki/Chinese_remainder_theorem?oldid=701807201 *Contributors:* AxelBoldt, Matthew Woodcraft, CYD, Bryan Derksen, Zundark, Taw, Taral, PierreAbbat, Stevertigo, Michael Hardy, Meekohi, Zeno Gantner, Jebba, Darkwind, Charles Matthews, Dcoetzee, Dysprosia, Fuzheado, Shizhao, Robbot, Lowellian, Ojigiri~enwiki, Davidcannon, Giftlite, DavidCary, Lupin, MSGJ, Dratman, Python eggs, DemonThing, David Battle, Icairns, Bluefoxicy, Shahab, DonDiego, Goochelaar, Shlomif, El C, Nickj, Scott Ritchie, Oleg Alexandrov, Mindmatrix, Drostie, Mpatel, Dionyziz, X127, Gisling, Marudubshinki, Kesla, Qwertyca, Jmcc150, Mathbot, DVdm, Algebraist, YurikBot, RobotE, Dmharvey, RussBot, Michael Slone, KSmrq, Mikeblas, Kompik, Arthur Rubin, Josh3580, SmackBot, RDBury, BeteNoir, Reedy, Bluebot, Kurykh, Bazonka, Nbarth, DHN-bot~enwiki, Thomasyen, DMacks, Black Carrot, Dr. Crash, Andrei Stroe, Wtwilson3, Shushanwen, Vanished user 8ij3r8jwefi, Newone, CRGreathouse, WLior, Thijs!bot, Mentifisto, Jj137, Salgueiro~enwiki, Rbb l181, Dricherby, Stuart Morrow, David Eppstein, Error792, JoergenB, Connor Behan, Quanticle, Mendevel, Glrx, Trusilver, Fruits Monster, Your mind17, LordAnubisBOT, Policron, Typometer, VolkovBot, Pleasantville, PMajer, TXiKiBoT, Plclark, Wykypydya, Sapphic, Arcfrk, PericlesofAthens, SieBot, Da Joe, Die Mensch-Maschine, OKBot, DrTJJ, ClueBot, Binksternet, PipepBot, Alexbot, Franklin.vp, Marc van Leeuwen, Druckles, Protonk, LaaknorBot, Newfraferz87, Lightbot, Legobot, Luckas-bot, Yobot, Fraggle81, Charleswallingford, AnomieBOT, Jim1138, LlywelynII, Citation bot, ArthurBot, Xqbot, SassoBot, Fenris.kcf, CryptoBm, FrescoBot, Adrionwells, Jannaston, D'ohBot, Darij, Garald, Creatorlarryli, Kallikanzarid, Trappist the monk, Lotje, RjwilmsiBot, John of Reading, Vincent Semeria, Fly by Night, Doomhydra1098, Preetum, D.Lazard, Alcazar84, ClueBot NG, Wcherowi, Quandle, Nilram12, MerlIwBot, MC-CPO, Manoguru, Aisteco, Lieutenant of Melkor, Myna vajha, Heilmoli, Ranjith1610, Frosty, Bnd30, CaoWiki, Mjaiclin, Vieque, Rcrptmncr, Navstar55, Novanijntje, 新規作成, Antonella Perucca 1982, Anuj1123, ObviouslyNotASock and Anonymous: 133

14.2 Images

- **File:Disqvisitiones-800.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/e3/Disqvisitiones-800.jpg *License:* Public domain *Contributors:* ? *Original artist:* ?

14.3 Content license

-