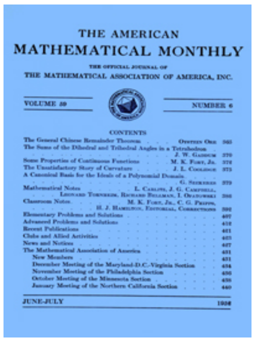

The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

# The General Chinese Remainder Theorem

Oystein Ore

**To cite this article:** Oystein Ore (1952) The General Chinese Remainder Theorem, The American Mathematical Monthly, 59:6, 365-370, DOI: 10.1080/00029890.1952.11988142

**To link to this article:** https://doi.org/10.1080/00029890.1952.11988142

Published online: 13 Mar 2018.

# THE GENERAL CHINESE REMAINDER THEOREM

OYSTEIN ORE, Yale University

**1. Introduction.** The Chinese remainder theorem, as one knows, is one of the most useful tools of elementary number theory. It presents a simple method of determining and representing the solution of a system of simultaneous congruences,

$$x \equiv a_i \pmod{m_i} \qquad (i = 1, 2, \cdots, k), \tag{1}$$

*provided the moduls $m_i$ are relatively prime in pairs.*

I have been unable to find mentioned anywhere in the mathematical literature the fact that it is possible to formulate a general Chinese remainder theorem, which includes the ordinary, but is valid without any restrictions on the moduls. This is the main result, Theorem 1, in the present paper. It has been expressed for rational integers only, but anyone familiar with the concepts of newer algebra will see how it may be formulated for ideals in quite general rings, so that this need not be elaborated. There have been added, however, some remarks on Abelian groups which appear quite naturally in this connection.

**2. The remainder theorem.** Let the system of congruences (1) be given where it is not assumed that the moduls are necessarily relatively prime. We recall that in this case the congruences do not always have a solution: the necessary and sufficient condition that they be solvable is that for all $i$ and $j$,

$$a_i \equiv a_j \pmod{d_{ij}}, \tag{2}$$

where we have put

$$d_{ij} = m_i \wedge m_j \tag{3}$$

for the greatest common divisor of the two moduls $m_i$ and $m_j$. When the conditions (2) are fulfilled the solution of (1) is uniquely determined for the least common multiple

$$M = m_1 \vee \cdots \vee m_k \tag{4}$$

as modul.

To formulate our theorem we need some further terminology. For each $i$ we shall write

$$A_i = m_1 \vee \cdots \vee m_{i-1} \vee m_{i+1} \vee \cdots \vee m_k$$

and

$$D_i = m_i \wedge A_i = d_{i,1} \vee \cdots \vee d_{i,i-1} \vee d_{i,i+1} \vee \cdots \vee d_{ik}.$$

The quotient of these two numbers is the integer

$$B_i = A_i/D_i. \tag{5}$$

This expression (5) for $B_i$ may be given various other forms by means of the well known identity

$$a \cdot b = (a \vee b) \cdot (a \wedge b). \tag{6}$$

First we have

$$B_i = \frac{A_i}{m_i \wedge A_i} = \frac{m_i \vee A_i}{m_i} = \frac{M}{m_i}. \tag{7}$$

This may be written

$$B_i = \frac{m_1 \vee m_i}{m_i} \vee \frac{m_2 \vee m_i}{m_i} \vee \cdots,$$

which again by (6) and (3) reduces to

$$B_i = \frac{m_1}{d_{1i}} \vee \frac{m_2}{d_{2i}} \vee \cdots. \tag{8}$$

After these preparations we state the main theorem:

THEOREM 1. *The solution of the simultaneous congruences* (1) *can be presented in the form*

$$x \equiv a_1 c_1 \frac{M}{m_1} + \cdots + a_k c_k \frac{M}{m_k} \pmod{M}, \tag{9}$$

*where the $c_i$ form a set of integers satisfying the condition*

$$c_1 \frac{M}{m_1} + \cdots + c_k \frac{M}{m_k} = 1. \tag{10}$$

*Proof.* We must first show that the numbers (7) have no common factor so that the indeterminate equation (10) has a solution set $\{c_i\}$. It suffices to show that for each prime $p$ at least one of the numbers $B_i$ is not divisible by $p$. Let $p^{\alpha_i}$ be the highest power of $p$ dividing $m_i$ and suppose for instance that $\alpha_1$ is the greatest among these exponents. Then $M$ is divisible exactly by $p^{\alpha_1}$ and $B_1$ is not divisible by $p$.

To prove that the expression $x$ in (9) actually is a solution of (1) let us examine it (mod $m_j$). When the congruence (2) is multiplied by $B_i$ we obtain

$$B_i a_i \equiv B_i a_j \pmod{d_{ij} \cdot B_i}.$$

But according to (8) the number $B_i$ is divisible by $m_j/d_{ij}$ so that we conclude that

$$B_i a_i \equiv B_i a_j \pmod{m_j}.$$

For each $i$ we multiply this congruence by $c_i$. When the resulting congruences are added one finds

$$x \equiv a_j(B_1c_1 + \cdots + B_kc_k) \pmod{m_j}$$

or, according to (10),

$$x \equiv a_j \pmod{m_j},$$

as desired.

It may be noticed that in the general solution (9) the multipliers for the residues $a_i$ are independent of the particular set of remainders involved in the system (1).

**3. Symmetric functions.** It is convenient to introduce operational symbols $\bigvee$ and $\bigwedge$ for taking the l.c.m. and g.c.d. of a set of numbers just as we use the sum sign $\sum$ and the product sign $\Pi$. Thus we write

$$\bigvee n_i = n_1 \vee \cdots \vee n_s$$
$$\bigwedge n_i = n_1 \wedge \cdots \wedge n_s$$

for the g.c.d. and l.c.m. of the numbers $n_i$.

As before let

$$m_1, m_2, \cdots, m_k \tag{11}$$

denote $k$ arbitrary positive integers. From these we form a system of *symmetric functions* by means of g.c.d. and l.c.m. operations, namely

$$\begin{aligned} M_r &= \bigvee m_{i_1} \wedge m_{i_2} \wedge \cdots \wedge m_{i_r} \\ N_r &= \bigwedge m_{i_1} \vee m_{i_2} \vee \cdots \vee m_{i_r} \end{aligned} \qquad (r = 1, 2, \cdots, k) \tag{12}$$

where, for each $r$, the choice of indices,

$$i_1, i_2, \cdots, i_r,$$

runs through all possible $C_{k,r}$ combinations of the numbers from 1 to $k$: in particular

$$M_1 = m_1 \vee \cdots \vee m_r,$$
$$N_1 = m_1 \wedge \cdots \wedge m_r.$$

From the distributive law for the g.c.d. and l.c.m. (see f. inst. Ore [**3**], chap. 5-4) one deduces from (12) that

$$M_r = N_{k-r+1}, \tag{13}$$

and it follows also fairly directly from the definitions (12) that

$$\begin{aligned} M_1 &\geqq M_2 \geqq \cdots \geqq M_k, \\ N_k &\geqq N_{k-1} \geqq \cdots \geqq N_1, \end{aligned} \tag{14}$$

where each term divides the preceding.

When $k$ is an odd number one obtains from (13) the self-dual identity

$$M_{(k+1)/2} = N_{(k+1)/2},$$

as has recently been pointed out by Mitrinovitch [1, 2].

These results can also be obtained quite simply by considering the exponents of the various powers of a prime $p$ which enter into the series of numbers (12). As before let $m_i$ be divisible exactly by $p^{\alpha_i}$; since our expressions are symmetric in the $m_i$ there is no limitation in assuming the notation such that

$$\alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_k.$$

Thus $M_i$ is divisible exactly by $p^{\alpha_i}$, that is by $p$ to the $i$-th largest exponent to which it occurs, and $N_i$ is divisible by exactly $p^{\alpha_{i-k+1}}$, that is, $p$ to the $(i-k+1)$-st highest exponent $\alpha$. Since this holds for every prime $p$ the relations (13) and (14) follow.

An easy consequence of this point of view is the formula

$$m_1 \cdot m_2 \cdots m_k = M_1 \cdot M_2 \cdots M_k, \tag{15}$$

which is a generalization of the simple relation (6). Both sides in (15) contain $p$ to a power with the exponent

$$\alpha_1 + \alpha_2 + \cdots + \alpha_k.$$

**4. Abelian groups.** The $k$-tuples

$$(x_i) = (x_1, x_2, \cdots, x_k) \tag{16}$$

with integral $x_i$ form an Abelian group under addition. When we suppose further that each $x_i$ is reduced modul $m_i$, we obtain the general finite Abelian group $A$ of the type

$$\mu = [m_1, m_2, \cdots, m_k], \tag{17}$$

that is, the group with $k$ basis elements of the respective orders $m_i$.

This representation of the Abelian group by its type is not unique since there may be several types giving the same group. To obtain a unique type representation one can split each $m_i$ into its prime power factors $p^{\alpha_i}$ and represent the type of $A$ by means of the *invariants*

$$\mu_i = [\cdots, p^{\alpha_i}, \cdots]. \tag{18}$$

A second way of obtaining a unique type representation is by means of the *elementary divisors* where one imposes the restriction on the type that each exponent shall be a divisor of the preceding. To construct this elementary divisor type from the invariant type (18) one can proceed as follows. For each prime $p$ one takes the highest invariant $p^{\alpha_i}$ and then one forms the product of these $p^{\alpha_i}$ over all the primes $p$ in (18). Next one takes the second highest invariants and their product, and so on. These products are evidently the symmetric functions $M_1, M_2, \cdots$ so that we can state:

THEOREM 2. *The elementary divisor type of an Abelian group of type* (17) *is*

$$\mu_e = [M_1, M_2, \cdots, M_k],$$

*where the numbers* $M_j$ *are the symmetric functions of the numbers* $m_i$.

From this point of view the formula (15) expresses only the fact that the order of the group is independent of the type representation.

Let us now consider what we may call the *residue k-tuples*

$$(a_i) = (a_1, a_2, \cdots, a_k). \tag{19}$$

These are the elements in $A$ for which the corresponding congruences (1) are solvable, that is, the sets of numbers for which the congruence conditions (2) are fulfilled. It is evident that these residue $k$-tuples (19) form a subgroup, the *residue group* $R$ of $A$. But since the congruences (1) are solvable in this case, each $a_i$ may be replaced by the same $x$ so that the residue group $R$ is simply the subgroup of $A$ consisting of all $k$-tuples

$$(x) = (x, x, \cdots, x)$$

in which all components may be taken to be the same. We notice that the order of $R$ is $M_1$.

Finally one may say that two $k$-tuples $(x_i)$ and $(y_i)$ in $A$ are *residue equivalent* if their difference is a residue $k$-tuple (19). The residue equivalence classes also form a group, the *residue difference group* $D$ isomorphic to the difference group $A-R$ (quotient group $A/R$). The order of this group is

$$\frac{m_1 \cdots m_k}{M_1} = M_2 \cdots M_k,$$

and we leave it to the reader to verify that its elementary divisors are actually

$$M_2, M_3, \cdots, M_k.$$

Instead of taking the additive group $A$ one could have considered the multiplicative group $A'$ consisting of those $k$-tuples in (16) in which each component $x_i$ is relatively prime to its corresponding modul. The type of this group is

$$\mu' = [\phi(m_1), \cdots, \phi(m_k)]$$

where, as usual, $\phi$ denotes Euler's function. Here our symmetric functions $M_j(m_i)$ are replaced by $M_j(\phi(m_i))$. The order of the group may be written in several forms:

$$\begin{aligned} \phi(m_1) \cdots \phi(m_k) &= M_1(\phi(m_i)) \cdots M_k(\phi(m_i)) \\ &= \phi(M_1(m_i)) \cdots \phi(M_k(m_i)). \end{aligned} \tag{20}$$

These identities (20) are extensions of the simple rule

$$\phi(a)\cdot\phi(b) = \phi(a \vee b)\cdot\phi(a \wedge b) = (\phi(a) \vee \phi(b))\cdot(\phi(a) \wedge \phi(b)).$$

**Bibliography**

1. D. S. Mitrinovitch: Sur une propriété des opérations *max* et *min*, C. R. Acad. Sci., Paris, v. 232, 1951, pp. 286–287.
2. D. S. Mitrinovitch: Sur certaines relations de l'algèbre des ensembles, Ibid., pp. 917–918.
3. Oystein Ore: Number theory and its history, New York, 1948, McGraw-Hill Book Company.

# THE SUMS OF THE DIHEDRAL AND TRIHEDRAL ANGLES IN A TETRAHEDRON*

J. W. GADDUM, National Bureau of Standards, Los Angeles, California

There is no theorem on the sum $S$ of the dihedral angles in a tetrahedron analogous to the theorem that the sum of the angles in a triangle is $\pi$ radians. Furthermore, a little experimentation shows that the sum is not a constant. However, bounds are known. It is well known that the sum of the three dihedral angles around any vertex is between $\pi$ and $3\pi$, from which it follows immediately that $S$ is between $2\pi$ and $6\pi$. These are the best bounds the writer has been able to find in the literature.

The principal result of this note is to show that $S$ is between $2\pi$ and $3\pi$, and that these bounds cannot be improved. Since $T$, the sum of the trihedral angles, is given by $T=2S-4\pi$, this also gives best bounds on $T$. (One would expect these results to be well known and the writer would appreciate information on this point. In any event, they do not appear to be readily accessible and the elementary proofs given here may be of value.)

We first prove a lemma about spherical triangles.

LEMMA. *If $x$ is a point interior to a spherical triangle $abc$, then $ax+bx+cx \leqq ab+bc+ac$.*

*Proof.* Extend $ax$, $bx$, $cx$, intersecting $bc$, $ac$, and $ab$, respectively in $p$, $q$, $r$. Then $cx+ax-ar \leqq cx+xr \leqq br+bc$. Hence $cx+ax \leqq ar+br+bc=ab+bc$. Similarly, $ax+bx \leqq bc+ac$, and $cx+bx \leqq ab+ac$. Adding and dividing by 2, $ax+bx+cx \leqq ab+bc+ac$.

The proof is clearly valid for plane triangles as well.

Proceeding to consider the theorem, given any tetrahedron, let us take an interior point $O$ and drop perpendiculars $r_1$, $r_2$, $r_3$, $r_4$ to the faces. Now the six dihedral angles of the tetrahedron are supplementary, respectively, to the six

* The preparation of this paper was sponsored (in part) by the Office of the Air Comptroller, USAF.