J. Korean Math. Soc.
Vol. 11, No. 1, 1974

THE CHINESE REMAINDER THEOREM

BY P. RAMANKUTTY

The classical Chinese Remainder Theorem in the context of rings and comaximal ideals is usually stated and proved under the hypothesis that the ring contains a multiplicative identity; often the additional restriction of commutativity is also imposed. Although it may not seem to be much of a restriction to assume the existence of the identity, it is not necessary to do so. The existence of the identity makes it trivially possible to express any given element of the ring as a product of any finite number of elements of the ring (not all factors being necessarily distinct); but this type of factorization can fail if the ring contains no identity. (e. g: The ring of even integers.) Furthermore a ring in which the above factorization property holds need not necessarily contain an identity. (e. g: The Boolean ring of all finite subsets of an infinite set).

This note presents an extension of the Chinese Remainder Theorem with neither commutativity nor the existence of the identity assumed.

THEOREM. *Let R be a ring and $A_1, \cdots, A_n$ comaximal ideals in R. Given elements $x_1, \cdots, x_n$; $z_1, \cdots, z_n$ in R there exists an element x in R such that $x \equiv x_i \prod_{\substack{j=1 \\ j \neq i}}^{n} z_j \pmod{A_i}$ for all $i=1, 2, \cdots, n$.*

DEFINITION. $A_1, \cdots, A_n$ are comaximal iff $i \neq j$ implies $A_i + A_j = R$.

Proof. First we assert that for each i there exists an element $y_i \in R$ such that $y_i \equiv \prod_{\substack{j=1 \\ j \neq i}}^{n} z_j \pmod{A_i}$ and $y_i \equiv 0 \pmod{A_j}$ for $j \neq i$. Clearly, it is sufficient to prove this assertion for $i=1$. For each $j \geq 2$, since $A_1 + A_j = R$, there exist $r_j \in A_1$ and $a_j \in A_j$ such that $z_j = r_j + a_j$. Let $y_1 = a_2 a_3 \cdots a_n$. Then $y_1 \equiv 0 \pmod{A_j}$ for $j \neq 1$, and $\prod_{j=2}^{n} z_j = \prod_{j=2}^{n} (r_j + a_j) = b_1 + y_1$ where $b_1 \in A_1$ so that $y_1 \equiv \prod_{i=2}^{n} z_j \pmod{A_1}$. This proves the assertion. Now let $x = \sum_{i=1}^{n} x_i y_i$. Since $y_i \equiv 0 \pmod{A_j}$ for $j \neq i$, it follows that $x \equiv x_i y_i \pmod{A_i}$ and the proof of the theorem is complete.

REMARK 1. The above result is an extension of the Chinese Remainder Theorem even if R contains an identity 1; however in this case setting $z_i = 1$ for each i, the usual version results.

REMARK 2. If each element of R can be expressed as a product of two elements of R then the converse of the above theorem is also true. Let us call a ring R *factorizable* iff for each $a \in R$ there exist b, c in R such that $a = bc$. It is immediate that if R is

Received by the editors Jan. 5, 1974.

factorizable then for each $a\in R$ and for each positive integer n there exist elements $a_1, \cdots, a_n$ in R such that $a=a_1a_2\cdots a_n$.

THEOREM 2. *Let R be a factorizable ring and $A_1, \cdots, A_n$ ideals in R. If for each set of elements $x_1, \cdots, x_n$; $z_1, \cdots z_n$ in R there exists an element x in R such that $x\equiv x_i \prod_{\substack{j=1\\ j\neq i}}^{n} z_j$ (mod A_i) for $i=1, \cdots, n$, then $A_1, \cdots, A_n$ are comaximal.*

Proof. Clearly, it is sufficient to prove that $A_1+A_2=R$. Let $y\in R$ and let $y_1, \cdots, y_n$ be elements of R such that $y=y_1y_2\cdots y_n$. Take $x_1=y_1y_2$, $x_2=y_1$, $x_3, \cdots, x_n$ arbitrary, $z_1=y_2^2-y_2$, and $z_i=y_i$ for $i=2, \cdots n$. By hypothesis there exists $x\in R$ such that $x\equiv x_1z_2z_3, \cdots, z_n$ (mod A_1) and $x\equiv x_2z_1z_3\cdots z_n$ (mod A_2). Writing $z_3z_4\cdots z_n=z$, the above congruences are $x\equiv y_1y_2^2z$ (mod A_1) and $x\equiv y_1(y_2^2-y_2)z$ (mod A_2).

Hence $(y_1y_2^2z-x)+(x-y_1(y_2^2-y_2)z) \in A_1+A_2$. This is the same as: $y_1y_2z\equiv A_1+A_2$ i. e. $y\in A_1+A_2$. Since $y\in R$ is arbitrary, the proof is complete.

References

[1] Barshay, J. *Topics in ring theory*, W. A. Benjamin, New York, 1969.
[2] Kaplansky, I. *Commutative rings*, Allyn & Bacon, Boston 1970.
[3] Lang, S. *Algebra*, Addison-Wesley, Reading 1965.
[4] Northcott, D. *Lessons on rings, modules and multiplicities*, Cambridge University Press, 1968.

University of Auckland