Journal of Pure and Applied Algebra 24 (1982) 221–226
North-Holland Publishing Company



# CHINESE RINGS

Karl Egil AUBERT and Istvàn BECK

*Department of Mathematics, University of Oslo, Blindern, Norway*

Communicated by H. Bass
Received 4 April 1981

## 1. Introduction

In a commutative ring $R$ with an identity element one can consider a multiplicative congruence which is coarser than the *classical* congruence modulo an ideal $\mathfrak{a}$ in $R$. Forming the factor ring $\bar{R} = R/\mathfrak{a}$ we declare $b$ and $c$ in $R$ as *canonically* congruent modulo $\mathfrak{a}$ whenever these two elements give rise to residue classes $\bar{b}, \bar{c}$ which generate the same principal ideal $(\bar{b}) = (\bar{c})$ in $\bar{R}$. We use the term 'canonical' because this congruence may be characterized as the unique coarsest *multiplicative* congruence on $R$ with the property that any ideal $\mathfrak{b} \supset \mathfrak{a}$ is a union of congruence classes. We shall denote the canonical congruence modulo $\mathfrak{a}$ by $b \equiv c\ (\mathfrak{a})$ whereas the classical congruence is, as usual, denoted by $b \equiv c \pmod{\mathfrak{a}}$.

Specializing to the ring $\mathbb{Z}$ of integers we have the following suggestive interpretation: the integers $a$ and $b$ are canonically congruent modulo $n$ iff the greatest common divisor of $a$ and $n$ equals the greatest common divisor of $b$ and $n$.

The aim of the present paper is to investigate for which rings the Chinese Remainder Theorem holds for a finite collection of canonical congruences which are compatible in an obvious sense. In contrast to the ordinary Chinese Remainder Theorem for classical congruences, this poses a non-trivial problem. Whereas *two* compatible, classical congruences always have a solution this is not the case for two canonical congruences even in a unique factorization domain like $\mathbb{Z}[x, y]$. We shall say that $R$ is a *Chinese ring* if, given elements $a, b \in R$ and ideals $\mathfrak{a}, \mathfrak{b} \subset R$ such that $a \equiv b\ (\mathfrak{a}+\mathfrak{b})$ there exists an element $c \in R$ such that $c \equiv a\ (\mathfrak{a})$ and $c \equiv b\ (\mathfrak{b})$. Although we shall not be able to give a complete characterization of Chinese rings we shall show that they include all Bezout rings, Dedekind domains and local rings as well as finite products and factors of such rings.

0022-4049/82/0000–0000/$02.75 

## 2. The Chinese Remainder Theorem in ideal systems

The above definition of a canonical congruence in a ring is just a special case of a kind of congruence which arises naturally in the theory of ideal systems. To every ideal $A$ in an ideal system on the commutative monoid $D$ there is associated a canonical congruence which may be characterized as the unique coarsest congruence on $D$ such that every ideal containing $A$ is a union of congruence classes. More explicitely, we may define this congruence by putting $b \equiv c\ (A)$ whenever $(A, b) = (A, c)$ (where ( ) denotes ideal generation) or with a different notation: $A + \{b\} = A + \{c\}$. (For basic definitions concerning ideal systems see [1] where a slightly different notation is used.)

We shall say that the Chinese Remainder Theorem for $n$ canonical congruences (abbreviated $\mathrm{CRT}_n$) holds for an ideal system on the monoid $D$ if the following property is satisfied: Given $n$ ideals $A_1, \ldots, A_n$ and $n$ elements $a_1, \ldots, a_n$ in $D$ such that $a_i \equiv a_j\ (A_i + A_j)$ there exists an element $a \in D$ such that $a \equiv a_i\ (A_i)$ for $i = 1, 2, \ldots, n$. It was proved in [2] that $\mathrm{CRT}_n$ holds for all $n$ if and only if $\mathrm{CRT}_2$ holds and the lattice of ideals is distributive - which in turn was shown to be equivalent to $\mathrm{CRT}_3$.

We can formulate a slightly different $\mathrm{CRT}_n$-condition exclusively in terms of ideals by replacing the above elements $a_1, \ldots, a_n$ by ideals and also ask for an *ideal solution* instead of the above element solution $a$. We shall in this case speak of the *ideal version* of $\mathrm{CRT}_n$. (By writing $B \equiv C\ (A)$ we simply mean $A + B = A + C$.) If the lattice of ideals is modular we shall speak of a *modular* ideal system.

**Lemma 1.** *The ideal version of* $\mathrm{CRT}_2$ *is satisfied in any modular ideal system, meaning that in any such system two compatible congruences will have an ideal solution. This ideal solution may be chosen to be finitely generated in case we are dealing with the usual element version of the* $\mathrm{CRT}_2$*-condition.*

**Proof.** The first part of the lemma is a direct consequence of the fact that in a general lattice $L$, the $\mathrm{CRT}_2$-condition for the 1-system of lattice ideals in $L$ is equivalent to the modularity of $L$ and also to the additivity of the 1-system in $L$ (see [1]). For the second part of the lemma, let $b, c, B, C$ be given subject to the compatibility condition $b \equiv c\ (B + C)$. By the first part of the lemma there exists an ideal $A$ such that $B + A = B + \{b\}$ and $C + A = C + \{c\}$. Since an ideal system is assumed to be of finite character we have a finite number of elements $a_i, a_j' \in A$, $b_r \in B$ and $c_s \in C$ such that $b \in (a_1, \ldots, a_m, b_1, \ldots, b_n)$ and $c \in (a_1', \ldots, a_k', c_1, \ldots, c_t)$ (where ( ) denotes ideal generation). By putting $F = (a_1, \ldots, a_m, a_1', \ldots, a_k')$ we shall have $B + F = B + \{b\}$ and $C + F = C + \{c\}$ as desired.

## 3. Chinese rings

We have defined a Chinese ring as a commutative ring with an identity element in which any two compatible canonical congruences possess an element solution.

**Lemma 2.** *The family of Chinese rings is closed under finite products and under factor formation.*

**Proof.** Let $R = R_1 \times \cdots \times R_n$ be a direct product of Chinese rings and assume that $(a_1, \ldots, a_n) \equiv (b_1, \ldots, b_n)$ $(\mathfrak{a} + \mathfrak{b})$ where $a_i, b_i \in R_i$ and $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $R$. It is clear that any ideal in $R$ is a product of ideals in the factors $R_i$, $\mathfrak{a} = \prod \pi_i(\mathfrak{a}) = \prod \mathfrak{a}_i$, at the same time as $a_i \equiv b_i$ $(\mathfrak{a}_i + \mathfrak{b}_i)$, the latter being a consequence of the relation

$$\prod \mathfrak{a}_i + \prod \mathfrak{b}_i = \prod (\mathfrak{a}_i + \mathfrak{b}_i). \tag{3.1}$$

Since each $R_i$ is Chinese we have elements $c_i \in R_i$ such that $c_i \equiv a_i$ $(\mathfrak{a}_i)$ and $c_i \equiv b_i$ $(\mathfrak{b}_i)$. The element $c = (c_1, \ldots, c_n) \in R$ then solves the original canonical congruences in $R$.

The second part of the lemma is obvious. It says that any homomorphic image of a Chinese ring is Chinese.

The following characterization of Chinese rings is quite useful.

**Lemma 3.** *A ring $R$ is Chinese if and only if for given elements $x, y, r, s \in R$ there exists an element $z \in R$ such that*

$$(x - ry, z) = (y - sx, z) = (x, y). \tag{3.2}$$

**Proof.** Assume first that $R$ is Chinese and put $\mathfrak{a} = (x - ry)$, $\mathfrak{b} = (y - sx)$ in which case $\mathfrak{a} + \mathfrak{b} \subset (x, y)$. Then $\mathfrak{a} + (y) = (x, y) = \mathfrak{b} + (x)$ and also $\mathfrak{a} + \mathfrak{b} + (y) = (x, y) = \mathfrak{a} + \mathfrak{b} + (x)$ which implies $x \equiv y$ $(\mathfrak{a} + \mathfrak{b})$. By $\mathrm{CRT}_2$ there exists $z \in R$ such that $z \equiv y$ $(\mathfrak{a})$ and $z \equiv x$ $(\mathfrak{b})$, i.e. $(\mathfrak{a}, z) = (\mathfrak{a}, y) = (x, y)$ and $(\mathfrak{b}, z) = (\mathfrak{b}, x) = (x, y)$ as required in (3.2).

Assume conversely that (3.2) holds. From a given compatibility condition $x \equiv y$ $(\mathfrak{a} + \mathfrak{b})$ where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $R$ we derive relations $x = a_1 + b_1 + ry$ and $y = a_2 + b_2 + sx$ with $a_1, a_2 \in \mathfrak{a}$, $b_1, b_2 \in \mathfrak{b}$ and $r, s \in R$. Putting $x' = x - a_1$ and $y' = y - b_2$ we obtain $x' = x - a_1 = b_1 + ry = b_1 + r(y' + b_2) = b + ry'$ with $b \in \mathfrak{b}$ and $y' = y - b_2 = a_2 + sx = a_2 + s(x' + a_1) = a + sx'$ with $a \in \mathfrak{a}$. Applying (3.2) to the elements $x', y', r, s$ there exists an element $z$ such that $(x' - ry', z) = (y' - sx', z) = (x', y') = (x', a) = (y', b)$ or $(b, z) = (a, z) = (x', y') = (x', a) = (y', b)$ from which follows $z \equiv x'$ $(\mathfrak{a})$ and $z \equiv y'$ $(\mathfrak{b})$. Combining this with the fact that $x' \equiv x \pmod{\mathfrak{a}}$ and $y' \equiv y \pmod{\mathfrak{b}}$, classically, and hence also canonically we obtain $z \equiv x$ $(\mathfrak{a})$ and $z \equiv y$ $(\mathfrak{b})$ as required.

**Theorem 1.** *The following types of rings are Chinese rings:*

(A) *Bezout rings,*

(B) *Dedekind domains,*

(C) *Local rings.*

**Proof.** *Case* A. We give two proofs. Since the lattice of ideals of a commutative ring $R$ is modular it follows from Lemma 1 that any two compatible congruences have a solution in terms of a finitely generated ideal - and hence an element solution in case $R$ is Bezout. On the other hand it is also clear that the relation (3.2) will be satisfied if we choose $z$ as a generator of the ideal $(x, y)$ in case $R$ is Bezout.

*Case* B. Let $a \equiv b$ $(\mathfrak{a}+\mathfrak{b})$ be given in $R$. If $\mathfrak{a}$ or $\mathfrak{b}$ is the zero-ideal in $R$ we shall have either $\mathfrak{a} \subset \mathfrak{b}$ or $\mathfrak{b} \subset \mathfrak{a}$ and $\mathrm{CRT}_2$ holds since we may choose the solution $c=a$ or $c=b$ respectively. We may therefore assume that both $\mathfrak{a}$ and $\mathfrak{b}$ are different from the zero-ideal, hence also $\mathfrak{a} \cap \mathfrak{b} \neq (0)$ since $R$ is an integral domain. By the Dedekind property the classical factor ring $R/\mathfrak{a} \cap \mathfrak{b}$ is a principal ideal ring and by Lemma 1 there exists an ideal $\mathfrak{c}$ in $R$ such that $\mathfrak{a}+\mathfrak{c}=\mathfrak{a}+\{a\}$ and $\mathfrak{b}+\mathfrak{c}=\mathfrak{b}+\{b\}$. Passing to the factor ring modulo $\mathfrak{a} \cap \mathfrak{b}$ the ideal $\mathfrak{c}$ is converted into a principal ideal $(\bar{c})$, $\bar{c} \in R/\mathfrak{a} \cap \mathfrak{b}$ and it is clear that $c$ represents a solution to the two given canonical congruences.

*Case* C. We shall show that (3.2) holds for a suitably chosen $z \in R$ in case $R$ is local. There are two possibilities:

(1) $r$ is a unit. Then $z=x$ will do.

(2) $r$ is not a unit, i.e. $r \in \mathfrak{m}$ (maximal ideal in $R$).

In this case we put $z=y-sx+x$ which gives the relation $(y-sx, z)=(x, y)$. Furthermore the ideal $(x-ry, y-sx+x)$ contains $x-ry+r(y-sx+x)=x(1-rs+r)$ and thus contains $x$ since $1-rs+r$ is a unit. Hence it also contains $y-sx+x+(s-1)x=y$ thereby completing the proof of the theorem.

Let a Dedekind *ring* be a commutative ring (with possible zero-divisors) such that any of its proper ideals may be written as a product of prime ideals. Such a ring is characterized by the fact that it is a direct product of a finite number of Dedekind *domains* and a principal ideal ring (see [3, p. 558]). Invoking Lemma 2 and reminding the reader of the basic fact that any commutative Artinian ring is a product of a finite number of local (Artinian) rings we thus get:

**Corollary 1.** *Any finite product of homomorphic images of Bezout rings, Dedekind domains and local rings is Chinese. In particular, Dedekind rings and Artinian rings are Chinese rings.*

We also note the following

**Corollary 2.** *The following types of rings have a Chinese Remainder Theorem for any finite number of canonical congruences:*

(1) *Principal ideal rings,*

(2) *Bezout rings,*

(3) *Dedekind domains (or rings),*

(4) *Any finite direct product of homomorphic images of rings of the types* (1), (2) *and* (3).

**Proof.** According to Theorem 1 (and Corollary 1) these types of rings are all Chinese. By the general result mentioned in Section 2 (and proved in [2]) it therefore suffices to show that they are also *arithmetical* (i.e. have a distributive ideal lattice). Since it is well known (and easily verified) that a ring is arithmetical if and only if its localizations at prime ideals are arithmetical, (1) follows from the fact that in a local principal ideal ring the Krull intersection theorem implies that the ideals are totally ordered under inclusion and hence form a distributive lattice. It is well known that Dedekind domains are arithmetical and so are Bezout rings, as was shown in [4]. Finally, the class of arithmetical rings is closed under finite direct products and under factor formation (i.e. under homomorphic images). The first part of this claim follows from (3.1) together with the similar relation $\prod \mathfrak{a}_i \cap \prod \mathfrak{b}_i = \prod (\mathfrak{a}_i \cap \mathfrak{b}_i)$. whereas the second part is obvious.

It follows from this corollary that Dedekind rings in the above sense as well as Von Neumann regular rings have a Chinese Remainder Theorem for canonical congruences.

## 4. Unique factorization domains need not be Chinese

In view of the quite comprehensive classes of Chinese rings mentioned above one might perhaps believe that every commutative ring with an identity element is Chinese. A crucial test-case is here formed by certain unique factorization domains, namely by polynomial rings over the ring of integers $\mathbb{Z}$. As a first result in this direction we may note the following consequence of Lemma 3.

**Proposition.** *If every polynomial ring $\mathbb{Z}[X, Y, U, V]$ in four variables over the integers were Chinese, then any commutative ring would be Chinese.*

**Proof.** If $\mathbb{Z}[X, Y, U, V]$ were Chinese, then, by Lemma 3, there would exist a $z \in \mathbb{Z}[X, Y, U, V]$ such that

$$(X - UY, z) = (Y - VX, z) = (X, Y).$$

Given four elements $x, y, r, s$ in a general ring $R$ we get a ring homomorphism $\phi : \mathbb{Z}[X, Y, U, V] \to R$ by sending $X, Y, U, V$ to $x, y, r, s$ respectively and $\phi(z)$ will according to Lemma 3 represent a solution to the two given canonical congruences and $R$ is hence Chinese.

However, every commutative ring is *not* Chinese and we need not go as far as *four* variables to prove this.

**Theorem 2.** *$\mathbb{Z}[x_1, x_2, \ldots, x_n]$ is not Chinese for $n \geq 2$.*

**Proof.** Due to the latter part of Lemma 2 we may limit ourselves to the ring $\mathbb{Z}[x, y]$. Put $\mathfrak{a}=(x)$, $\mathfrak{b}=(3x-5y)$, $a=y$, $b=x-2y$. Then $a\equiv b\ (\mathfrak{a}+\mathfrak{b})$, but in spite of this we shall show that there is no $z$ solving the relevant congruences, i.e. satisfying the relations

$$(x, z)=(x, y), \tag{4.1}$$

$$(3x-5y, x)=(3x-5y, x-2y). \tag{4.2}$$

Assume that $z$ is written in the form $z=f_0(x)+f_1(x)y+f_2(x)y^2+\cdots$ and consider the ring homomorphism $f(x, y)\to\widetilde{f(x, y)}=f(0, y)$ from $\mathbb{Z}[x, y]$ to $\mathbb{Z}[y]$. Applying

$$\tilde{z}=f_0(0)+f_1(0)\tilde{y}+\cdots \tag{4.3}$$

to the relation (4.1) we obtain $(\tilde{z})=(\tilde{y})$ which together with (4.3) gives $f_0(0)=0$, $f_1(0)=\pm 1$ and $f_i(0)=0$ for $i\geq 2$. This means that

$$z=\varepsilon_1 y+xf(x, y) \tag{4.4}$$

with $\varepsilon_1=\pm 1$ and $f(x, y)\in\mathbb{Z}[x, y]$.

A similar restriction on $z$ may be derived from (4.2). Putting $\mathbb{Z}[x, y]=\mathbb{Z}[3x-5y, x-2y]=\mathbb{Z}[u, v]$ and noting that $u=3x-5y$ and $v=x-2y$ are algebraically independent, we can rewrite (4.2) as $(u, z)=(u, v)$, obtaining with this change of variables the same relation as in (4.1). By the same procedure as above we thus arrive at

$$z=\varepsilon_2(x-2y)+(3x-5y)g(x, y) \tag{4.5}$$

with $\varepsilon_2=\pm 1$ and $g(x, y)\in\mathbb{Z}[x, y]$.

Comparing (4.4) and (4.5) and putting $x=0$ we derive the contradiction $5\mid(\varepsilon_1+2\varepsilon_2)$.

Among the types of rings about which one could ask whether they are Chinese or not are the Prüfer domains and the semilocal rings. A particular case which ought to be settled is of course $\mathbb{Z}[x]$. A general characterization of Chinese rings might conceivably be given in term of their modules.

## References

[1] K.E. Aubert, Ideal systems and lattice theory II, J. Reine Angew. Math. 298 (1978) 32–42.

[2] K.E. Aubert and G. Gismarvik, Chinese Remainder Theorems in ideal systems (submitted for publication).

[3] N. Bourbaki, Commutative Algebra, Chapter VI (Hermann, Paris and Addison Wesley, Reading, MA, 1972).

[4] C.U. Jensen, Arithmetical Rings, Acta Math. Acad. Sci. Hungar. 17 (1966) 115–123.