CHINESE REMAINDER THEOREMS IN IDEAL SYSTEMS

by

K.E. Aubert and G. Gismarvik

1. Introduction. The original Chinese remainder theorem is a theorem of elementary number theory which under an evident necessary condition affirms the simultanous solvability of a finite set of congruences. This theorem has given rise to offspring in various directions. Among its arithmetical descendants should be counted several types of approximation theorems in valuation theory. More direct (but less arithmetical) analogues of the Chinese remainder theorem have been considered within such fields as lattice theory [4], lattice ordered groups [5] and universal algebra [3].

The purpose of the present paper is to show that the general theory of ideal systems offers a convenient framework for the treatment of various Chinese remainder theorems. It should be noted that the canonical congruences (or equivalences) which are here considered in ideal systems are not generalizations of the usual congruences of ring theory. Hence our development leads to some new results and some new problems also in the case of rings. On the one hand it will turn out that there exist commutative rings such that the Chinese remainder theorem with respect to two canonical congruences does not hold. On the other hand we shall prove (in several different ways) that the Chinese remainder theorem for any finite number of canonical congruences holds in a Dedekind domain. In the case of the ring $\mathbb{Z}$

of integers this result has a simple number-theoretic interpretation in terms of greatest common divisors. The general problem of characterizing those commutative rings (or domains) where the Chinese remainder theorem holds for any finite number of canonical congruences seems to be of interest. The results of this paper show only that in the case of a domain the solution to this problem lies somewhere between 'Dedekind' and 'Prüfer'.

In contradistinction to the case of rings the general notion of a canonical equivalence specializes in the case of lattices to the usual equivalence modulo a lattice ideal. This leads to a rather neat characterization of the difference between modularity and distributivity in lattices: A lattice is modular if and only if the Chinese remainder theorem holds for any <u>two</u> canonical equivalences and it is distributive if and only if the same theorem holds for any <u>three</u> (or more) canonical equivalences. This result can be used to give a very simple proof of the aforementioned Chinese remainder theorem in a Dedekind domain.

As another easy application we consider a Chinese remainder theorem for canonical congruences relative to the usual notion of ideal in a commutative monoid. In this situation it turns out that the Chinese remainder theorem for two canonical congruences is equivalent to their permutability which in turn is equivalent to the monoid being totally preordered by divisibility - and this condition assures that the Chinese remainder theorem holds for any finite number of canonical congruences.

The present exposition will also provide some new insight into the relationship between the Chinese remainder theorem for ideal systems and other concepts from the theory of ideal systems like additivity, modularity, permutability, distributivity and the intersection

property.

The term 'ideal system' needs some clarification. In fact we shall here rather work within the wider framework of 'generalized ideal systems' ('ideal systems without continuity axiom'). We could even go one step further and consider closure systems with non-void intersections in the same way as it was done in [1]. Indeed, Chinese remainder theorems are essentially non-multiplicative theorems which concern equivalences rather than congruences. But since all our applications will be to ideal systems (with or without continuity axiom) we shall not bother about the extra generality on this occasion.

2. Canonical equivalences in generalized ideal systems. For basic definitions concerning ideal systems the reader is referred to [1] or [2]. If we drop the continuity axiom ($AB_x \subset (AB)_x$) from the definition of an ideal system, we get a generalized ideal system. To any x-ideal A_x in the generalized ideal system (D, x) there is associated an equivalence by putting $b \equiv c(A_x)$ whenever $(A_x,b)_x = (A_x,c)_x$ (also written $A_x + \{b\} = A_x + \{c\}$). This is the unique coarsest equivalence relation in D with the property that any x-ideal B_x containing A_x is a union of equivalence classes. We call this equivalence the canonical equivalence associated with A_x. These canonical equivalences are all congruences if the continuity axiom is satisfied, but all the canonical equivalences in (D,x) may be congruences without (D,x) satisfying the continuity axiom. The exact condition which is needed in order that all canonical equivalences be congruences, is that the quotient $A_x : b$ is a union of equivalence classes modulo A_x.

We note that $b \equiv c(A_x)$ implies $b \equiv c(B_x)$ for any $B_x \supset A_x$. On the other hand it is not true in general that $b \equiv c(A_x)$ and

$b \equiv c(C_x)$ imply $b \equiv c(A_x \cap C_x)$. We say that (D,x) satisfies the intersection property if this implication is always true. One sees immediately that any generalized ideal system with a distributive lattice of x-ideals, has the intersection property (Theorem 6 in [1]).

3. The Chinese remainder theorem. Let (D,x) be a generalized ideal system. We denote the x-ideal generated by the union of A_x and B_x by $A_x + B_x$. We shall say that the Chinese remainder theorem for n canonical equivalences holds in (D,x) - or that the condition $CRT_n(x)$ (or simply CRT_n) holds in (D,x) - if the following property is satisfied: Given n x-ideals $A_x^{(1)}, A_x^{(2)}, \ldots, A_x^{(n)}$ and n elements $a_1, a_2, \ldots, a_n \in D$ such that $a_i \equiv a_j (A_x^{(i)} + A_x^{(j)})$ there exists an element $a \in D$ such that $a \equiv a_i (A_x^{(i)})$ for $i = 1,2,\ldots n$. We note that the condition $a_i \equiv a_j (A_x^{(i)} + A_x^{(j)})$ certainly is a necessary condition for the existence of a simultanous solution to the n canonical equivalences in question. For $a \equiv a_i (A_x^{(i)})$ and $a \equiv a_j (A_x^{(j)})$ imply $a \equiv a_i (A_x^{(i)} + A_x^{(j)})$ and $a \equiv a_j (A_x^{(i)} + A_x^{(j)})$ and hence by transitivity the given compatibility condition.

Theorem 1. (Chinese remainder theorem for generalized ideal systems). The condition CRT_n $(n \geq 3)$ holds in a generalized ideal system if and only if CRT_2 holds and the lattice of ideals is distributive.

Proof: It is clear that $CRT_n \Rightarrow CRT_m$ whenever $m < n$ (by considering the case $A_x^{(m)} = A_x^{(m+1)} = \ldots = A_x^{(n)}$ and $a_m = a_{m+1} = \ldots = a_n$). In particular $CRT_n \Rightarrow CRT_2$ for every $n \geq 3$. We shall next show that CRT_3 implies that the lattice of x-ideals of (D,x) is distributive. Assume that

$$3.1. \qquad a_1 \in (A_x + B_x) \cap (A_x + C_x) \quad \text{and} \quad a_2 \in B_x \cap C_x$$

We consider the two canonical equivalences

3.2. $\qquad a \equiv a_1(A_x)$

and

3.3. $\qquad a \equiv a_2(B_x \cap C_x)$

The equivalence 3.3. is equivalent to the conjunction of the two equivalences

3.4. $\qquad a \equiv a_2(B_x)$

and

3.5. $\qquad a \equiv a_2(C_x)$

Clearly 3.4. and 3.5. follow from 3.3. On the other hand $a_2 \in B_x \cap C_x$ which together with 3.4. and 3.5. implies $a \in B_x \cap C_x$, hence 3.3. That we really have a solution a to the two equivalences 3.2. and 3.3. is a consequence of the fact that the equivalent system 3.2., 3.4. and 3.5. according to 3.1. satisfies the compatibility requirements

$$a_1 \equiv a_2(A_x+B_x), \quad a_1 \equiv a_2(A_x+C_x) \quad \text{and} \quad a_2 \equiv a_2(B_x+C_x)$$

and hence has a solution according to CRT_3. When $a \in B_x \cap C_x$ is combined with 3.2., we conslude that $a_1 \in A_x + (B_x \cap C_x)$ which proves the distributivity of the ideal lattice.

We prove the converse by induction. Since we assume CRT_2 this starts the induction. Suppose next that $a_i \equiv a_j(A_x^{(i)} + A_x^{(j)})$ for $i,j = 1,2,\ldots n$. By induction we can assume that there exists an element a' such that

3.6. $\qquad a' \equiv a_i(A_x^{(i)}), \quad i = 1,2,\ldots n-1$

Combining 3.6. with $a_i \equiv a_n(A_x^{(i)} + A_x^{(n)}) \quad i = 1,2,\ldots n-1$, and

using transitivity we obtain $a' \equiv a_n(A_x^{(i)} + A_x^{(n)})$. Since (D,x) is supposed to have a distributive ideal lattice, and this implies the intersection property, we get

$$a' \equiv a_n(\bigcap_{i=1}^{n-1}(A_x^{(i)} + A_x^{(n)}))$$

and again by distributivity

$$3.7. \qquad a' \equiv a_n(A_x^{(n)} + \bigcap_{i=1}^{n-1} A_x^{(i)})$$

By CRT_2 and 3.7. there exists an element $a \in D$ such that

$$3.8. \qquad a \equiv a_n(A_x^{(n)})$$

and

$$3.9. \qquad a \equiv a'(\bigcap_{i=1}^{n-1} A_x^{(i)})$$

From 3.9. we obtain $a \equiv a'(A_x^{(i)})$ for $i = 1,2,\ldots n-1$ and hence by 3.6. $a \equiv a_i(A_x^{(i)})$ for $i = 1,2,\ldots n-1$. This together with 3.8. completes the proof of the theorem.

We note the following

Corollary. In a generalized ideal system CRT_n holds for all n if and only if CRT_3 holds.

4. Commutative rings. We shall first take a look at the content of Theorem 1 in the case of ordinary ideals (here also called d-ideals) in a commutative ring R. In the presence of an identity element the relationship between the classical and the canonical congruence modulo a d-ideal A_d in R is particularly simple to formulate. In this case the canonical equivalence modulo A_d is a congruence (with respect to multiplication) giving rise to a residue class monoid

which is nothing but the monoid of all principal ideals in the ordinary residue class ring R/A_d. Otherwise expressed: Two elements in R are canonically congruent (d-congruent) modulo A_d if and only if they give rise to associate elements in the residue class ring R/A_d (whereas they give rise to identical elements if they are congruent in the usual sense).

Somewhat surprisingly the difficulty in characterizing those rings which satisfy CRT_n in the case of canonical congruences resides essentially in the case $n = 2$. Whereas the classical Chinese remainder theorem holds trivially for two congruences in any commutative ring, we shall now prove the following

Theorem 2. There are commutative rings in which the Chinese remainder theorem for two canonical congruences does not hold.

Proof: (The following example emerged during some clarifying discussions with I. Fleischer). Let $\mathbb{Q}$ denote the additive group of rational numbers and let $R = \mathbb{Q} \oplus \mathbb{Q}$ be the ring with zero multiplication whose underlying additive group is a direct sum of two copies of $\mathbb{Q}$. Consider the two ideals $A = \mathbb{Z} \oplus \{0\}$ and $B = \{0\} \oplus \mathbb{Z}$ in R. Then $A + B = \mathbb{Z} \oplus \mathbb{Z}$ and the two elements $(\frac{1}{3}, \frac{2}{9})$ and $(\frac{1}{3}, \frac{8}{9})$ in R are canonically equivalent modulo $A + B$, i.e.

$$(\mathbb{Z} \oplus \mathbb{Z}, (\tfrac{1}{3}, \tfrac{2}{9})) = (\mathbb{Z} \oplus \mathbb{Z}, (\tfrac{1}{3}, \tfrac{8}{9}))$$

(This because $4(\frac{1}{3}, \frac{2}{9}) = (1,0) + (\frac{1}{3}, \frac{8}{9})$ and $7(\frac{1}{3}, \frac{8}{9}) = (2,6) + (\frac{1}{3}, \frac{2}{9})$.)

If $CRT_2(d)$ were valid in R there would hence exist an element $(a,b) \in R$ such that

$$4.1. \qquad (\mathbb{Z} \oplus \{0\}, (a,b)) = (\mathbb{Z} \oplus \{0\}, (\tfrac{1}{3}, \tfrac{2}{9}))$$

and

$$4.2. \qquad (\{0\} \oplus \mathbb{Z}, (a,b)) = (\{0\} \oplus \mathbb{Z}, (\tfrac{1}{3}, \tfrac{8}{9}))$$

From 4.1. we deduce $b = m \cdot \frac{2}{9}$ and $\frac{2}{9} = nb$ with $m,n \in \mathbb{Z}$ hence $b = \pm\frac{2}{9}$. Similarly 4.2. gives $a = \pm\frac{1}{3}$. It is clear, however, that 4.2. can not be satisfied for these values of a and b since this would require $n \pm \frac{2}{9} = \frac{8}{9}$ with $n \in \mathbb{Z}$.

When it comes to positive results, it is natural to start with the ring $\mathbb{Z}$ of integers which along with the classical Chinese remainder theorem also posesses a completely analogous property relative to canonical congruences. These latter congruences have the following simple number-theoretic content: The integers a and b are canonically congruent modulo n if the greatest common divisor of a and n is the same as the greatest common divisor of b and n.

Theorem 3. The Chinese remainder theorem holds in $\mathbb{Z}$ for any finite number of canonical congruences.

Proof: Since the ideal lattice of $\mathbb{Z}$ is distributive, it suffices according to Theorem 1 to show that $CRT_2(d)$ is verified in $\mathbb{Z}$. Denoting the greatest (positive) common divisor of the integers $a_1, a_2, \ldots, a_k$ by $(a_1, a_2, \ldots, a_k)$ the CRT_2-condition amounts to the following in the principal ideal domain $\mathbb{Z}$: If a,b and m,n are two pairs of integers such that

$$4.3. \qquad (m,n,a) = (m,n,b)$$

then there exists an integer c such that

$$4.4. \qquad (m,a) = (m,c) \text{ and } (n,b) = (n,c)$$

It is possible to give a reformulation of 4.3. and 4.4. if we look at an element ($\neq 0$) in $\mathbb{Z}$ as a divisor, i.e. as an integer-valued

(positive) function with finite support defined over the set P consisting of all primes. With a corresponding functional notation 4.3. is then equivalent to the conjunction of the two implications

4.5. $\quad a(p) < (m \wedge n)(p) \Rightarrow a(p) = b(p)$

and

4.6. $\quad a(p) \geq (m \wedge n)(p) \Rightarrow b(p) \geq (m \wedge n)(p)$

where $p \in P$ and $m \wedge n$ denotes the infimum of the two functions m and n. The conclusion 4.4. in CRT_2 then asserts the existence of a divisor c defined on P such that the following four implications hold.

4.7. $\quad a(p) < m(p) \Rightarrow c(p) = a(p)$

4.8. $\quad a(p) \geq m(p) \Rightarrow c(p) \geq m(p)$

4.9. $\quad b(p) < n(p) \Rightarrow c(p) = b(p)$

4.10. $\quad b(p) \geq n(p) \Rightarrow c(p) \geq n(p)$

By distinguishing the following four cases (i) $a(p) < m(p)$ and $b(p) < n(p)$ (ii) $a(p) < m(p)$ and $b(p) \geq n(p)$ (iii) $a(p) \geq m(p)$ and $b(p) < n(p)$ and (iv) $a(p) \geq m(p)$ and $b(p) \geq n(p)$ it is easy to see that we in each case can make a choice of the value $c(p)$ which is consistent with the restrictions imposed by the implications 4.5. - 4.10. (putting respectively $c(p) = a(p) = b(p)$, $c(p) = a(p)$, $c(p) = b(p)$ and $c(p) = (a \vee b)(p)$ in the four cases (i) - (iv)). In case some of the integers a, b, m, n happen to be equal to zero, we make the usual convention $0(p) = -\infty$ so as to extend the above proof to all cases.

Although the above proof of Theorem 3 is simple enough, it does not fully exploit the technique of localization. In fact CRT_2 for

canonical congruences is always valid in a valuation ring - the ideals being totally ordered with respect to inclusion in this case. Indeed, if $a \equiv b(A_d + B_d)$ and $B_d \subset A_d$ then the two canonical congruences $c \equiv a(A_d)$ and $c \equiv b(B_d)$ will have $c = b$ as a solution. In case of the ring $\mathbb{Z}$ this means that with the above notation we only need to distinguish the two cases $m(p) \geq n(p)$ and $m(p) \leq n(p)$ corresponding to the solutions $c(p) = a(p)$ and $c(p) = b(p)$ respectively - and this furnishes a second and shorter proof of Theorem 3.

On the basis of the above proofs we can easily establish the following more general result:

Theorem 4. The Chinese remainder theorem holds in a Dedekind domain for any finite number of canonical congruences.

Proof: By Theorem 1 and the distributivity of the ideal lattice of a Dedekind domain it is again sufficient to prove $CRT_2(d)$. Hence, let the d-ideals A_d, B_d and the elements a, b be given such that $a \equiv b(A_d + B_d)$. In case at least one of the ideals A_d, B_d is the zero ideal, we shall have $A_d \subset B_d$ or $B_d \subset A_d$ and according to the second proof of Theorem 3 $CRT_2(d)$ is valid in this case. We may thus assume that both A_d and B_d are different from the zero ideal in the given Dedekind domain R. Then $A_d \cap B_d \neq (0)$ and $R/A_d \cap B_d$ is a principal ideal domain. According to the reasoning in the proof of Theorem 3 we can find a divisor C_d (interpreted as an ideal) such that $A_d + C_d = A_d + \{a\}$ and $B_d + C_d = B_d + \{b\}$ (where the $+$-sign corresponds to the infimum in the divisor interpretation). Passing to the residue class ring modulo $A_d \cap B_d$ the ideal C_d turns into a principal ideal $\bar{C}_d = (\bar{c})$ with $c \in R$. It is then clear that c satisfies $c \equiv a(A_d)$ and $c \equiv b(B_d)$ and this completes the proof.

5. Monoids. A particularly simple case is $x = s$, i.e. usual ideals in a commutative monoid D where ideal generation is given by $A_s = DA$ assuming that D has an identity element. We shall say that the commutative monoid D is a valuation monoid if D is totally preordered by divisibility. This amounts to saying that the family of s-ideals is totally ordered under inclusion.

Whereas the s-ideals of a monoid D always form a distributive lattice under inclusion (because they form a sublattice of the lattice of all subsets of D) the condition $CRT_2(s)$ only holds in a very special situation:

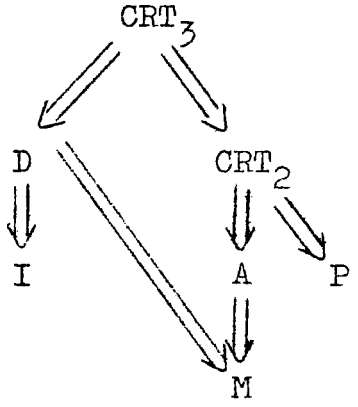
Theorem 5. In a commutative monoid D the following conditions are equivalent

1. $CRT_2(s)$
2. $CRT_n(s)$ for any $n \geq 3$
3. Any two canonical s-congruences in D are permutable
4. D is a valuation monoid

Proof: In view of Theorem 1 the equivalence of 1. and 2. is clear. Furthermore the implication 1 => 3 is contained in Theorem 4 in [2] and 3 => 4 follows thus: If D is not a valuation monoid, there exist two s-ideals A_s and B_s in D such that $A_s \not\subset B_s$ and $B_s \not\subset A_s$. Denoting the canonical congruence which is associated with the s-ideal A_s by $\theta(A_s)$ we shall clearly have $a\theta(A_s)\theta(B_s)b$ for $a \in A_s - B_b$ and $b \in B_s - A_s$. This because $a\theta(A_s)c$ and $c\theta(B_s)b$ for any $c \in A_s \cap B_s$. On the other hand $a\theta(B_s)\theta(A_s)b$ signifies that there exists an element $c \in D$ such that $a\theta(B_s)c$ and $c\theta(A_s)b$. By the choice of a and b this entails $c \notin A_s \cup B_s$. Thus a and c

are two elements which are both outside of B_s and s-congruent modulo B_s, hence associates, contradicting the fact that the s-ideal A_s "separates" a and c. In order to prove 4 => 1 assume that $A_s \subset B_s$ are two s-ideals in the valuation monoid D. In this case $a \equiv b(A_s + B_s)$ implies that either both a and b are in B_s or neither of them is in B_s. In the former case a will be a solution of the two relevant congruences, and in the latter case either a or b can be used as a solution.

6. Conditions related to CRT_n. Before giving a brief account of the Chinese remainder theorem in lattices, we shall look a little bit into the relationship between CRT_n for generalized ideal systems and other conditions occurring in the theory of ideal systems like additivity (abbreviated by A), modularity of the lattice of ideals (M), permutability of canonical equivalences (P), distributivity of the lattice of ideals (D), and the intersection property (I). We have the following diagram of implications within the framework of generalized ideal systems (or even closure systems with non-void intersections).



Among these implications A => M and D => I are proved in [1]. The implications CRT_3 => D and CRT_3 => CRT_2 are part of the proof of Theorem 1 and CRT_2 => P is proved in [2] (Theorem 4).

Finally $CRT_2 \Rightarrow A$ is also easily established: Let $c \in A_x + B_x$ and $b \in B_x$. By CRT_2 there exists an element $d \in D$ such that $d \equiv c(A_x)$ and $d \equiv b(B_x)$. The latter equivalence implies that $d \in B_x$ and the additivity then becomes a consequence of the former equivalence.

Apart from the possibilities $P \Rightarrow CRT_2$, $P \Rightarrow A$ or $P \Rightarrow M$ (which we leave unsettled) there are in general no other implications between these conditions than those which are indicated in the above diagram. For this the following list of counterexamples will suffice

$I \not\Rightarrow M$ (The system of lattice ideals in the 5-element non-modular lattice)

$CRT_2 \not\Rightarrow I$ (The system of lattice ideals in the 5-element modular but non-distributive lattice)

$D \not\Rightarrow P$ (The s-system in a monoid which is not a valuation monoid)

$D \not\Rightarrow A$ (The example given in the proof of Theorem 8 in [1])

$A \not\Rightarrow P$ (The s-system in a monoid which is not a valuation monoid)

The conditions CRT_2, additivity, modularity and permutability (P) are closely related to each other and become identical under various conditions imposed on the given closure system. In the case of lattice ideals (see the next section and [2]) all these conditions are equivalent. We have also seen that CRT_2 is equivalent to permutability for the s-system in a monoid. Another situation where these concepts show a tendency to coincide, is given by the couple generated closure systems. A closure system (D,x) is said to be

couple generated if to a given closed set (x-ideal) A_x in D and a given element $a \in A_x$ there always exists an element $b \in A_x$ such that $(a,b)_x = A_x$. The traces of the d-ideals in a Dedekind domain R on the multiplicative monoid $R^* = R - \{0\}$ form a couple generated ideal system in R^*.

Theorem 6. The following properties are equivalent for a couple generated generalized ideal system.

1. The Chinese remainder theorem for two canonical equivalences (CRT_2)
2. Additivity
3. Modularity of the ideal lattice

Proof: We shall establish the theorem by means of the following sequence of implications: 1 => 2 => 3 => 2 => 1. The two first implications are part of the above diagram and 3 => 2 was proved for couple generated closure systems in [1]. Hence, we only need to prove 2 => 1. Assume $c_1 \equiv c_2(A_x + B_x)$. By additivity this implies the existence of elements c' and c" such that

6.1. $c_1 \equiv c'(A_x)$ with $c' \in B_x + \{c_2\}$

6.2. $c_2 \equiv c''(B_x)$ with $c'' \in A_x + \{c_1\}$

Writing out the meaning of 6.1. and 6.2. we conclude that c' and c" both belong to $C_x = (A_x + \{c_1\}) \cap (B_x + \{c_2\})$. Since $c' \in C_x$ we get by modularity that

6.3. $C_x = (A_x + \{c_1\}) \cap C_x = (A_x + \{c'\}) \cap C_x = (A_x \cap C_x) + \{c'\}$

Similarly $C_x = (B_x \cap C_x) + \{c''\}$. Let $a \in A_x \cap B_x$. By the basic assumption there exists an element c such that $C_x = (a,c)_x$. Com-

bined with 6.1. and 6.3. this gives $A_x + \{c\} = A_x + C_x = A_x + \{c'\} = A_x + \{c_1\}$ or $c \equiv c_1(A_x)$. In the same way we obtain $c \equiv c_2(B_x)$ and hence CRT_2.

Theorem 6 (combined with Theorem 1) gives us a new proof of Theorem 4 since the non-zero d-ideals in a Dedekind domain form a distributive lattice and their traces on the monoid R^* form a couple generated ideal system.

7. Lattices. We shall here content ourselves with a brief mention of the case of lattices and refer the reader to [2] for a more thorough treatment. Chinese remainder theorems in lattices were appearantly first considered by V.K. Balachandran in [4] Dealing exclusively with distributive lattices the main problem of characterizing those lattices for which CRT_n holds, was not approached in [4]. According to Theorem 1 it is sufficient to consider the two cases $n = 2$ and $n = 3$.

Spelling out the general notion of a canonical equivalence in the case of the system of ideals (here called 1-ideals) in a lattice L, we arrive at the following more suggestive formulation:

Two elements $b, c \in L$ are canonically equivalent modulo the 1-ideal A_1 if and only if there exists an element $a \in A_1$ such that $b \cup a = c \cup a$.

In contradistinction to d-ideals in rings the canonical equivalence associated with an 1-ideal thus reduces to the familiar notion which has already been considered in [4] and elsewhere.

We have shown that CRT_2 implies the modularity of the ideal lattice. In case of the 1-system in a lattice L this means that $CRT_2(1)$ implies the modularity of L itself. Conversely, if L

is modular, the 1-system in L is additive (Theorem 3 in [1]) and hence satisfies CRT_2 according to the proof of Corollary 1 of Theorem 4 in [2]. Combining this with the above Theorem 1, we obtain the following

Theorem 7. The Chinese remainder theorem holds for two (resp. three or more) canonical equivalences in a lattice L if and only if L is modular (resp. distributive).

We note that Theorem 7 gives us still another approach to Theorem 4 by considering the family of d-ideals in a Dedekind domain as a distributive (and hence modular) lattice under set-inclusion. Theorem 7 gives us a solution of the relevant congruences in terms of d-ideals and this ideal solution is converted into an element solution by passing to a residue class ring in the same manner as in the proof of Theorem 4.

References

[1] K.E. Aubert, Ideal systems and lattice theory I, Algebra Universalis 1, (1971), 204-213.

[2] K.E. Aubert, Ideal systems and lattice theory II, forthcoming.

[3] K.A. Baker and A.F. Pixley, Polynomial interpolation and the Chinese remainder theorem for algebraic systems, Math. Zeitschr. 143 (1975), 165-174.

[4] V.K. Balachandran, The Chinese remainder theorem for distributive lattices, The Journal of the Indian Math. Soc. 13 (1949), 76-80.

[5] T. Nakano, A theorem on lattice ordered groups and its application to valuation theory, Math. Zeitschr. 83 (1964), 140-146.