ACTA ARITHMETICA
XLIV (1984)

Irreducible disjoint covering systems

by

IVAN KOREC (Bratislava)

An operation called splitting will be defined on the disjoint covering system (DCS) of congruence classes on Z. It will allow us to decompose every natural DCS to some full systems Z_p, p a prime, of congruence classes modulo p. This decomposition of natural DCS corresponds to Z-trees in [4] (where further references also can be found). Irreducible DCS, to which every (general) DCS can be decomposed, are introduced. Several infinite classes of irreducible DCS will be constructed. They will make possible to find infinitely many non-natural DCS.

1. Notation and basic notions. The symbol Z will denote the set of integers. The letter D will denote the greatest common divisor and l.c.m. the least common multiple; $a|b$ will denote: a divides b. For integers $n > 0$, a, the symbol $a(\mathrm{mod}\ n)$ will denote the congruence class $\{a+nx;\ x \in Z\}$. Although $0 \leqslant a < n$ is usual, an arbitrary a in the term $a(\mathrm{mod}\ n)$ is allowed; for example, $13(\mathrm{mod}\ 7) = -1(\mathrm{mod}\ 7) = 6(\mathrm{mod}\ 7)$.

The intersection of any two congruence classes $X = a(\mathrm{mod}\ m)$, $Y = b(\mathrm{mod}\ n)$ is either empty or a congruence class. The first case never takes place if m, n are relatively prime. Further, if X is a subset of Y then the modulus n of Y divides the modulus m of X.

The system

$$(1.1) \qquad a_1(\mathrm{mod}\ n_1),\ a_2(\mathrm{mod}\ n_2),\ \ldots,\ a_k(\mathrm{mod}\ n_k)$$

will be called *disjoint covering system* (abbreviated: DCS) if every integer belongs to exactly one of the classes (1.1). More formally, a DCS is a partition of Z into finitely many congruence classes (we always assume that these classes are given in (1.1) without repetition). The integers $n_1, \ldots, n_k$ will be called *moduli* of (1.1) and their least common multiple $N = \mathrm{l.c.m.}\ (n_1, \ldots, n_k)$ will be called the *common modulus* of (1.1).

The partition $\{Z\}$ is usually excluded from the consideration but it will be considered as a (degenerated) DCS in the present paper. Therefore some theorems on DCS's must be slightly modified. For example, a well-known necessary condition on the modulus of a DCS (1.1) is

$$D(n_i, n_j) > 1 \quad \text{for every } i, j \in \{1, \ldots, k\},\ i \neq j. \tag{1.2}$$

(Here "$i \neq j$" had to be added.) The condition (1.2) follows from the fact that the intersection of any two congruence classes with relatively prime moduli is nonempty.

For every positive integer n denote by Z_n or $Z(n)$ the partition of Z into the congruence classes modulo n (the symbol $Z(n)$ is sometimes used to avoid double indices). In particular,

$$Z_2 = \{0(\text{mod } 2), 1(\text{mod } 2)\} \quad \text{and} \quad Z_1 = \{0(\text{mod } 1)\} = \{Z\}.$$

The number of elements of a set X will be denoted by $\operatorname{card}(X)$.

2. Definition of IDCS and splitting. Now we shall define irreducible DCS and the operations of splitting which allows us to obtain all DCS from the irreducible ones.

DEFINITION 2.1. (a) Let S_2, S_3 be DCS, let $b(\text{mod } d) \in S_2$ and let S_1 be the DCS (1.1). We shall say that S_3 *arises by the b-splitting of S_2 by S_1*, and write $S_3 = \operatorname{Split}(S_2, b, S_1)$ if

$$S_3 = (S_2 - \{b(\text{mod } d)\}) \cup \{b + a_i d(\text{mod } n_i d);\ i \in \{1, \ldots, k\}\}.$$

(b) We shall write $\operatorname{Split}(S_1, a_1, S_2, a_2, S_3)$ instead of $\operatorname{Split}(\operatorname{Split}(S_1, a_1, S_2), a_2, S_3)$, and analogously for a greater number of splittings. Further, we define $\operatorname{Split}(S) = S$ for every DCS S.

The last part of this definition will be necessary, e.g. in Theorem 2.4.

EXAMPLES 2.2. $\operatorname{Split}(Z_2, 1, Z_3)$ consists of $0(\text{mod } 2)$, $1(\text{mod } 6)$, $3(\text{mod } 6)$, $5(\text{mod } 6)$, and $\operatorname{Split}(Z_2, 1, Z_3, 1, Z_2)$ consists of $0(\text{mod } 2)$, $1(\text{mod } 12)$, $7(\text{mod } 12)$, $3(\text{mod } 6)$, $5(\text{mod } 6)$.

On the other hand, $\operatorname{Split}(Z_3, 1, Z_2)$ consists of $0(\text{mod } 3)$, $1(\text{mod } 6)$, $4(\text{mod } 6)$, $2(\text{mod } 3)$ and hence $\operatorname{Split}(Z_2, 1, \operatorname{Split}(Z_3, 1, Z_2))$ consists of $0(\text{mod } 2)$, $1(\text{mod } 6)$, $3(\text{mod } 12)$, $9(\text{mod } 12)$, $5(\text{mod } 6)$.

We can easily see that for every DCS S and every integer a

$$\operatorname{Split}(Z_1, a, S) = \operatorname{Split}(S, a, Z_1) = S.$$

DEFINITION 2.3. A DCS (1.1) will be called *reducible* if there is $X \subseteq \{1, \ldots, k\}$, $1 < \operatorname{card}(X) < k$, such that $\bigcup \{a_i(\text{mod } n_i);\ i \in X\}$ is a congruence class. A DCS (1.1) will be called *irreducible disjoint covering system* (abbreviated: IDCS) if $k > 1$ and the DCS (1.1) is not reducible.

For example, Z_4 is reducible, because $0(\text{mod } 4) \cup 2(\text{mod } 4) = 0(\text{mod } 2)$. The partition Z_1 is neither IDCS nor reducible DCS, analogously as the integer 1 is neither prime nor composite.

Now we can formulate the decomposition theorem.

THEOREM 2.4. *For every DCS S there are IDCS $S_1, \ldots, S_n$ and integers $b_1, \ldots, b_n$ such that*

$$S = \operatorname{Split}(Z_1, b_1, S_1, \ldots, b_n, S_n). \tag{2.4}$$

Proof. We use the induction with respect to $\operatorname{card}(S)$. For $S = Z_1$ we choose $n = 0$. If S is irreducible we choose $n = 1$, b_1 arbitrary and $S_1 = S$. Now let S be reducible. Then there is a subset T of S such that $1 < \operatorname{card}(T) < \operatorname{card}(S)$ and the union of T is a congruence class $b(\text{mod } d)$. We may assume that T is a minimal subset with this property, i.e. for no $T_1 \subseteq T$, $1 < \operatorname{card}(T_1) < \operatorname{card}(T)$, $\bigcup T_1$ is a congruence class. Let T consist of the congruence classes (1.1). Then

$$\frac{a_1 - b}{d}\left(\text{mod } \frac{n_1}{d}\right), \ \ldots, \ \frac{a_k - b}{d}\left(\text{mod } \frac{n_k}{d}\right)$$

is an IDCS; denote it by S_n. The set $S' = (S - T) \cup \{b(\text{mod } d)\}$ is a DCS consisting of less than S congruence classes. Hence by the inductive assumption

$$S' = \operatorname{Split}(Z_1, b_1, S_1, \ldots, b_{n-1}, S_{n-1})$$

for some integers $b_1, \ldots, b_{n-1}$ and IDCS $S_1, \ldots, S_{n-1}$. However,

$$S = \operatorname{Split}(S', b, S_n),$$

and hence we have (2.4) for $b_n = b$. ∎

To obtain more comprehensive notation we can extend Definition 2.1 as follows.

DEFINITION 2.5. If S_1, S_2 are DCS and $X = \{b_1, \ldots, b_k\}$ is a finite set of integers such that b_i, b_j belong to different elements of S_1 whenever $i \neq j$, then we shall also write $\operatorname{Split}(S_1, X, S_2)$ or $\operatorname{Split}(S_1, \{b_1, \ldots, b_k\}, S_2)$ instead of

$$\operatorname{Split}(S_1, b_1, S_2, b_2, S_2, \ldots, b_k, S_2). \tag{2.5}$$

We shall also use $\operatorname{Split}(S_1, X_1, \ldots, S_k, X_k, S_{k+1})$ analogously to Definition 2.1(b).

The condition on $b_1, \ldots, b_k$ makes (2.5) independent on their order; hence $\operatorname{Split}(S_1, X, S_2)$ is defined correctly. (We can also imagine that the splittings in (2.5) are parallel.) The inequality $\operatorname{Split}(Z_2, 4, Z_2, 6, Z_2) \neq \operatorname{Split}(Z_2, 6, Z_2, 4, Z_2)$ shows that this condition cannot be omitted.

As an example of use of 2.5, notice that

$$\operatorname{Split}(Z_2, \{0, 1\}, \operatorname{Split}(Z_3, \{0, 2\}, Z_5), 2, Z_7)$$

denotes a DCS which consists of 28 congruence classes and has the common modulus 210.

The operation of splitting allows us to define a class of DCS which was intensively studied, see [1], [2], [3], [4].

DEFINITION 2.6. A DCS S will be called a *natural DCS* (abbreviated: NDCS) if there are integers $a_1, \ldots, a_k$ and positive integers $n_0, n_1, \ldots, n_k$ such that

$$S = \operatorname{Split}(Z(n_0), a_1, Z(n_1), \ldots, a_k, Z(n_k)).$$

Equivalently, a DCS is an NDCS if it arises by finitely many splittings from the DCS Z_k, $k = 1, 2, 3, \ldots$ The next example shows that in the decomposition (2.4) of a natural DCS also some non-natural IDCS can occur. Simultaneously it shows once more that the decomposition (2.4) of a DCS is not uniquely determined.

EXAMPLE 2.7. Let P be the DCS consisting of the following 13 congruence classes: 0, 4(mod 6); 1, 3, 5, 9(mod 10); 2(mod 15); 7, 8, 14, 20, 26, 27(mod 30) (P is derived from Porubský's example of a non-natural DCS, see [2].) Then

$$Z_{30} = \operatorname{Split}(P, \{0, 4\}, Z_5, \{1, 3, 5, 9\}, Z_3, 2, Z_2)$$

and simultaneously

$$Z_{30} = \operatorname{Split}(Z_2, \{0, 1\}, Z_3, \{0, 1, 2, 3, 4, 5\}, Z_5).$$

There are also further decompositions of Z_{30}.

3. Common modulus of IDCS. In this section, a simple necessary and sufficient condition for common modulus of IDCS will be proved. The natural IDCS will be fully described by Theorem 3.1, and then non-natural IDCS will be mainly studied. The first example of a non-natural DCS was given by Š. Porubský [2]. The example can be immediately used in the construction of several non-natural IDCS, all with the common modulus 30. N. Burshtein [1] also gave several examples of non-natural DCS, however they all were based on Porubský's example and lead to the same non-natural IDCS. Here an infinite set of non-natural IDCS will be constructed. For the sake of completeness the natural IDCS will also be described.

THEOREM 3.1. *An NDCS X is irreducible if and only if $X = Z_p$ for a prime p.*

Proof. If X is not of the form Z_k, then X is obviously reducible by the definition of NDCS. If $X = Z_{mn}$ for some $m > 1$, $n > 1$ then $1 < m < \operatorname{card}(X)$ and the union of m elements $ni(\text{mod } mn)$, $i = 1, \ldots, m$ is a congruence class. Therefore, X is reducible. Conversely, if k is a prime then elements of Z_k are maximal (proper) congruence classes, and hence Z_k is irreducible.

The parts (b) and (c) of the next lemma hold for every non-natural DCS. In part (a) the irreducibility is substantial; an example can be found in [1]; another example is $\operatorname{Split}(Z_3, 0, P)$ where P is from Example 2.7. The example Z_3 shows that non-naturality is substantial in (a), (b), (c); for (a), (c) also $\operatorname{Split}(Z_2, 0, Z_3)$ can be considered.

LEMMA 3.2. (a) *The greatest common divisor of all moduli of a non-natural IDCS is equal to 1.*

(b) *No modulus of a non-natural IDCS is a prime power.*

(c) *The common modulus of every non-natural IDCS has at least three prime divisors.*

Proof. (a) Let p be a prime divisor of all moduli of a DCS S, and let $S \neq Z_p$ (only here non-naturality is used). Every $i(\text{mod } p)$ $(i = 0, 1, \ldots, p-1)$ is the union of a subset X_i of S. Since $S \neq Z_p$, we have $\operatorname{card}(X_i) > 1$ for some i, and obviously $\operatorname{card}(X_i) < k$, which contradicts the irreducibility of S.

(b) If a prime power p^k is a modulus of an IDCS S then by (1.2) all moduli of S are multiples of p. Hence $S = Z_p$ by the first part of the proof, and S is natural, which contradicts the assumption.

(c) It easily follows from the first two parts. (For a reducible S, a non-natural IDCS S_i from (2.5) must be considered in the proof.)

THEOREM 3.3. *For a positive integer N, an IDCS with the common modulus N exists if and only if either N is a prime or N has at least three prime divisors.*

Proof. Let S be an IDCS with the common modulus N. If S is natural then N is a prime. If S is not natural then Lemma 3.2 implies that N has at least three prime divisors. Conversely, if N is a prime then N is the common modulus of the natural IDCS Z_N. It remains the case where N has at least three prime divisors.

Let $N = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ be the standard form of N, $p_1 < p_2 < \ldots < p_k$ and $k \geqslant 3$. Denote $N_i = N/p_i$ for $i = 1, \ldots, k$, and write

$$X_i = (N_i(\text{mod } p_i^{a_i})) \cap (i \cdot N_k(\text{mod } p_k^{a_k})) \quad \text{for} \quad i = 1, \ldots, k-1,$$
$$X_k = 0(\text{mod } p_1^{a_1} \cdot \ldots \cdot p_{k-1}^{a_{k-1}}).$$

The sets X_i $(i = 1, \ldots, k-1)$ are nonempty; hence they are congruence classes modulo $p_i^{a_i} \cdot p_k^{a_k}$; the set X_k is obviously a congruence class. These sets are pairwise disjoint. Indeed, if, for example, $X_i \cap X_j \neq \emptyset$ for some $1 \leqslant i < j \leqslant k-1$ then

$$(i \cdot N_k(\text{mod } p_k^{a_k})) \cap (j \cdot N_k(\text{mod } p_k^{a_k})) \neq \emptyset, \qquad p_k^{a_k} \mid (j-i) \cdot N_k;$$

hence $p_k \mid (j-i)$ which contradicts $0 < j-i < k < p_k$. Analogously, if $X_i \cap X_k \neq \emptyset$ for some $1 \leqslant i \leqslant k-1$ then $p_i^{a_i} \mid N_i$, a contradiction.

Since the congruence classes $X_1, \ldots, X_k$ are pairwise disjoint (and their moduli divide N), there is a DCS S with the common modulus N which contains all $X_1, \ldots, X_k$. The system S can be expressed in the form (2.4). We shall show that the common modulus of the IDCS S_1 is N. The common modulus M of S_1 obviously divides N. To finish the proof, we show that N also divides M.

Take arbitrary i, $1 \leqslant i \leqslant k-1$. The set X_i is contained in some $Y \in S_1$. Obviously,

$$Y = b(\mathrm{mod}\ p_i^u p_k^v) = \big(b(\mathrm{mod}\ p_i^u)\big) \cap \big(b(\mathrm{mod}\ p_k^v)\big)$$

for some $u \leqslant a_i$, $v \leqslant a_k$ and integer $b \in X$. Then we can obtain

$$Y = \big(N_i(\mathrm{mod}\ p_i^u)\big) \cap \big(i \cdot N_k(\mathrm{mod}\ p_k^v)\big).$$

If $u < a_i$ then $N_i \equiv 0(\mathrm{mod}\ p_i^u)$, and

$$Y \cap X_k = \big(0(\mathrm{mod}\ p_1^{a_1} \cdot \ldots \cdot p_{k-1}^{a_{k-1}})\big) \cap \big(i \cdot N_k(\mathrm{mod}\ p_k^{a_k})\big) \neq \emptyset$$

because the moduli are relatively prime. Hence $X_k \subseteq Y$ what gives $p_i^u p_k^v | p_1^{a_1} \cdot \ldots \cdot p_{k-1}^{a_{k-1}}$, $v = 0$, which contradicts Lemma 3.2 (b). Therefore $u = a_i$, which implies $p_i^{a_i} | M$ for arbitrary $i = 1, \ldots, k-1$.

It remains to prove $p_k^{a_k} | M$. Consider arbitrary $j \neq i$, $1 \leqslant j \leqslant k-1$ (the assumption $k \geqslant 3$ is used here). The set X_j is contained in an element

$$Y' = \big(N_j(\mathrm{mod}\ p_j^z)\big) \cap \big(j \cdot N_k(\mathrm{mod}\ p_k^w)\big)$$

of the set S_1. If $v < a_k$ and $w < a_k$ then $N_k \equiv 0(\mathrm{mod}\ p_k^v)$, $N_k \equiv 0(\mathrm{mod}\ p_k^w)$, and hence

$$Y \cap Y' = \big(N_i(\mathrm{mod}\ p_i^u)\big) \cap \big(N_j(\mathrm{mod}\ p_j^z)\big) \cap \big(0(\mathrm{mod}\ p_k^{\max(v,w)})\big) \neq \emptyset.$$

Therefore $Y = Y'$, which implies

$$p_i^u p_k^v = p_j^z p_k^w.$$

From that we have $u = 0$, $z = 0$ which contradicts Lemma 3.2 (b). Therefore, $v = a_k$ or $w = a_k$, and in both the cases $p_k^{a_k} | M$, which completes the proof.

No classification of IDCS will be made in the present paper. However, we shall show that there are IDCS which substantially differ from the IDCS contructed above.

THEOREM 3.4. *For every k there is an IDCS such that every modulus of it has at least k prime divisors.*

Proof. Let $k > 1$ be given. Choose $2k-1$ primes $p_1, \ldots, p_{2k-1}$ such that

$$\binom{2k-1}{k} \leqslant p_1 < p_2 < \ldots < p_{2k-1}.$$

The set $P = \{p_1, \ldots, p_{2k-1}\}$ has $r = \binom{2k-1}{k}$ subsets consisting of k elements. Let $n_1, \ldots, n_r$ be the products of elements of these sets, and $N = p_1 p_2 \cdot \ldots \cdot p_{2k-1}$. The congruence classes

$$i(\mathrm{mod}\ n_i), \quad i = 1, \ldots, r$$

are pairwise disjoint, and their moduli divide N. Hence there is a DCS S with the common modulus N which contains all these classes. Let S be expressed in the form (2.4). We shall show that every modulus m of S_1 has at least k prime divisors. Let, conversely, $b(\mathrm{mod}\ m) \in S_1$, and m have less than k prime divisors. Then there is i, $1 \leqslant i \leqslant r$ such that $D(m, n_i) = 1$. The congruence class $b(\mathrm{mod}\, m)$ has a nonempty intersection with $i(\mathrm{mod}\ n_i)$, and hence it must contain $i(\mathrm{mod}\ n_i)$. Therefore $m | n_i$, which contradicts $m > 1$ and $D(m, n_i) = 1$.

References

[1] N. Burshtein, *Exactly covering systems of congruences*, Ph. D. thesis, University of Tel Aviv, 1974.

[2] Š. Porubský, *Natural exactly covering systems of congruences*, Czech. Math. Journal 24 (1974), pp. 598–606.

[3] — *Results and problems on covering systems of residue classes*, Mitt. Math. Semin. Giessen, Heft 150, 1981, pp. 1–85.

[4] Š. Znám, *A survey of covering system of congruences*, Acta Math. Univ. Comen. 40–41 (1982), pp. 59–79.

Received on 14.6.1983
and in revised form on 15.11.1983 (1364)