Acta Math. Univ. Comenianae
Vol. LXIII, 1(1994), pp. 133–140

A NEW NECESSARY CONDITION FOR MODULI OF NON–NATURAL IRREDUCIBLE DISJOINT COVERING SYSTEM

I. POLÁCH

Abstract. A disjoint covering system $\mathbf{S} = (a_1 \pmod{n_1}, \dots, a_k \pmod{n_k})$ is said to be irreducible if the union of any of its r residue classes, $1 < r < k$, is not a residue class. An irreducible disjoint covering system is non-natural if not all its moduli are equal. The least common multiple of its moduli $n_1, \dots, n_k$ will be called the common modulus of $\mathbf{S}$. The main and most interesting result of this paper is Theorem 2.2 giving this neccesary condition: if p^α is a divisor of the common modulus of $\mathbf{S}$ (p a prime), then there exist at least 3 residue classes in $\mathbf{S}$ with the pairwise different moduli divisible by p^α. In the last section an example class of irreducible systems with the set of moduli containing exactly 4 elements is given.

1. Introduction and Basic Properties

Denote $\mathbf{Z}$ the set of all integers. By symbols gcd and lcm we mean the greatest common divisor and the least common multiple respectively. For any integers $n > 0$ and a the symbol $a \pmod{n}$ will denote the residue class $\{a + kn;\ k \in \mathbf{Z}\}$. The numbers a and n are called the residuum and modulus.

The system

$$\mathbf{S} = (a_1 \pmod{n_1}, \dots, a_k \pmod{n_k}) \tag{1}$$

of residue classes is said to be a **disjoint covering system** (abbreviated: DCS) if every integer belongs to exactly one residue class of $\mathbf{S}$ (in some papers it is called exactly covering system or simply exact cover). The number $m = \operatorname{lcm}(n_1, \dots, n_k)$ will be called **the common modulus** (sometimes called order of $\mathbf{S}$). For more details see references of survey papers by Znám [**6**] and Porubský [**4**].

We shall say z **is covered by** $a \pmod{n}$ if $z \in a \pmod{n}$ and analogously z **is covered by S** if there exists a class $a \pmod{n} \in \mathbf{S}$ such that z is covered by $a \pmod{n}$.

Complicated DCS can be usually obtained from simpler ones by replacing one residue class by a system of "smaller" residue classes (class $b \pmod{d}$ is replaced by

Received June 15, 1992; revised June 1, 1993.
1980 *Mathematics Subject Classification* (1991 *Revision*). Primary 10A10.
Key words and phrases. Disjoint covering system, irreducible disjoint covering system.

the system $\{b + a_i d \pmod{n_i d};\ a_i \pmod{n_i} \in \mathbf{S}\}$ obtained from DCS $\mathbf{S}$) see [**5**]. Korec in [**3**] introduced for this replacing a new operation called splitting (see also [**5**]):

Definition 1.1. Let $\mathbf{S}_2$, $\mathbf{S}_3$ be **DCS**-s, let $b \pmod{d} \in \mathbf{S}_2$ and $\mathbf{S}_1$ be the **DCS** (1). We shall say that $\mathbf{S}_3$ **arises by the** b**-splitting of** $\mathbf{S}_2$ **by** $\mathbf{S}_1$ if

$$\mathbf{S}_3 = (\mathbf{S}_2 - \{b \pmod{d}\}) \cup \{b + a_i d \pmod{n_i d};\ i \in \{1, \dots, k\}\}.$$

Disjoint covering systems that cannot be obtained from simpler ones are called irreducible DCS:

Definition 1.2. A DCS (1) is said to be **reducible** if there is $X \subset \{1, \dots, k\}$; $1 < \operatorname{card}(X) < k$ such that $\bigcup \{a_i \pmod{n_i};\ i \in X\}$ is a residue class.

A DCS (1) is called **irreducible disjoint covering system** (abbreviated: IDCS) if $k > 1$ and DCS (1) is not reducible.

A DCS obtained from $\{0 \pmod 1\}$ by splitting using disjoint covering systems of the form

$$\mathbf{R} = (0 \pmod{n}, \dots, n-1 \pmod{n}) \tag{2}$$

is called **natural DCS** (see [**5**]).

Korec in [**3**] proved that all natural IDCS are of the form (2), where n is a prime and gave some necessary conditions on non-natural IDCS .

Finally — symbol $\mu(\mathbf{S})$ will denote the set of all moduli of the DCS $\mathbf{S}$.

2. Necessary Condition for Non-Natural IDCS

Lemma 2.1. *Let* $\mathbf{S}$ *be a non-natural* IDCS (1), $m \pmod{n}$ *a residue class. Denote*

$$\mathbf{T} = \{a_i \pmod{n_i};\ a_i \pmod{n_i} \cap m \pmod{n} \neq \varnothing\}.$$

If $\mathbf{T} \subset \mathbf{S}$ *is a proper subsystem containing at least* 2 *residue classes, then there are residue classes* $a_s \pmod{n_s}$ *and* $a_t \pmod{n_t}$ *in* $\mathbf{T}$ *such that* $n_s \neq n_t$.

Proof. If all such residue classes had equal moduli, then the union of $\mathbf{T}$ would be a residue class $m \pmod{\gcd(n, n_i)}$. □

Theorem 2.2. *Let* $\mathbf{S}$ *be a non-natural* IDCS *and* p^α *a divisor of it's common modulus, where* p *is a prime. Then there exist three pairwise distinct moduli* n_i, n_j, n_k *such that*

$$p^\alpha \mid n_i \ \ \&\ \ p^\alpha \mid n_j \ \ \&\ \ p^\alpha \mid n_k.$$

Proof. Since the prime power p^α is a divisor of the least common multiple of all moduli, there exists at least one residue class $a_i \pmod{n_i} \in \mathbf{S}$ such that $p^\alpha \mid n_i$. Let n_i be the smallest modulus with this property. Denote $d = n_i/p$. Then

$$a_i \pmod{n_i} \subset a_i \pmod{d}.$$

$\mathbf{S}$ is covering, so for every integer $x \in a_i \pmod{d}$ there is an index $s = s(x)$ such that residue class $a_s \pmod{n_s}$ contains x.

Residue classes $a_s \pmod{n_s}$ and $a_i \pmod{d}$ are not disjoint since $x \in a_i \pmod{d}$ and $x \in a_s \pmod{n_s}$. So

$$\gcd(d, n_s) \mid (a_i - a_s).$$

If indices i, s are distinct, then the classes $a_i \pmod{n_i}$ and $a_s \pmod{n_s}$ are disjoint, so $\gcd(n_i, n_s) \nmid (a_i - a_s)$ and that is possible only if $p^\alpha \mid n_s$. Thus we have proved

(∗) Modulus n_s of such residue class $a_s \pmod{n_s}$ that $a_s \pmod{n_s} \cap a_i \pmod{d} \neq \emptyset$, is divisible by p^α.

If every $x \in a_i \pmod{d}$ were covered by an $a_s \pmod{n_s}$, with the modulus $n_s = n_i$ then by Lemma 2.1 the system $\mathbf{S}$ would be reducible, what contradicts the irreducibility of $\mathbf{S}$. So there exists a residue class $a_j \pmod{n_j}$ such that p^α divides n_j and $n_j \neq n_i$.

It remains now to find the third residue class $a_k \pmod{n_k}$ with a modulus distinct from n_i and n_j:

Consider the residue class $y \pmod{n_i}$, where $y \in a_i \pmod{d} \cap a_j \pmod{n_j}$. This class is a nonempty subset of $\mathbf{Z}$, so there is a set of residue classes

$$\mathbf{T} = (a_t \pmod{n_t};\ a_t \pmod{n_t} \cap y \pmod{n_i} \neq \varnothing) \subseteq \mathbf{S}$$

such that for every $x \in y \pmod{n_i}$ there is a class $a_t \pmod{n_t} \in \mathbf{T}$ covering x. Due to (∗) every modulus in $\mathbf{T}$ is divisible by p^α since $y \pmod{n_i}$ is a subset of $a_i \pmod{d}$. $\mathbf{T}$ contains at least 2 classes, because $a_j \pmod{n_j} \in \mathbf{T}$ and $n_i < n_j$ and so no class of $\mathbf{T}$ has modulus equal to n_i and so $\mathbf{T}$ cannot contain all the residue classes of $\mathbf{S}$. By Lemma 2.1 there is a residue class $a_t \pmod{n_t} \in \mathbf{T}$ such that $n_t \neq n_j$. □

Corollary 2.3. *The set of moduli $\mu(\mathbf{S})$ of any non-natural* IDCS *has at least* 4 *elements.*

Proof. By Lemma 3.2 of [**3**] the greatest common divisor of all moduli of $\mathbf{S}$ is 1. If a prime p is a divisor of common modulus of $\mathbf{S}$ then by Theorem 2.2 $\mu(\mathbf{S})$ has 3 distinct moduli divisible by p. So there must exist a modulus that is not divisible by p. □

From Lemma 3.2 of [**3**] we receive this special case:

Corollary 2.4. *Let* $\mathbf{S}$ *be a non-natural* IDCS *with the set of moduli* $\mu(\mathbf{S})$ *containing exactly four elements. Let* p^α *divide the common modulus. Then* p^α *divides exactly* 3 *moduli of* $\mu(\mathbf{S})$ *and* p *does not divide the last one.*

The Theorem 2.2 gives us more. If $\mu(\mathbf{S})$ has exactly four elements, then knowing the common modulus of $\mathbf{S}$ we can describe the set $\mu(\mathbf{S})$:

Corollary 2.5. *Let* $\mathbf{S}$ *be a non-natural* IDCS *with the set of moduli containing exactly four elements. Then*

$$\mu(\mathbf{S}) = \{d_1d_2d_3, d_1d_2d_4, d_1d_3d_4, d_2d_3d_4\},$$

where d_1, d_2, d_3, d_4 *are pairwise coprime and at most one of them is equal to 1 and* $d_1d_2d_3d_4$ *is equal to the common modulus.*

Proof. Let $\mu(\mathbf{S}) = \{b_1, b_2, b_3, b_4\}$. Denote

$$d_1 = \gcd(b_2, b_3, b_4); \quad d_2 = \gcd(b_1, b_3, b_4);$$
$$d_3 = \gcd(b_1, b_2, b_4); \quad d_4 = \gcd(b_1, b_2, b_3).$$

(i) The numbers d_1, d_2, d_3, d_4 are pairwise coprime, because if the prime p divides 3 distinct moduli, then it cannot divide the last one and so every prime p is divisor of at most one of the numbers d_1, d_2, d_3, d_4.

(ii) We will show that $b_4 = d_1d_2d_3$ (the proof of the equalities $b_1 = d_2d_3d_4$, $b_2 = d_1d_3d_4$, $b_3 = d_1d_2d_4$, is the same). From the notation and property (i) follows that $d_1d_2d_3$ divides b_1. If p^α divides b_1 then p^α must divide other two moduli b_j and b_k and so there must exist a divisor d_s ($s \in \{1, 2, 3\}$) divisible by p^α since d_1, d_2, d_3 are denoting the greatest common divisors of all triples of the moduli containing b_1.

(iii) We prove that at most one of the divisors d_1, d_2, d_3, d_4 is equal to 1. Let for example d_1, d_2 be equal to 1. Then due to (ii) there holds that $b_3 = d_4$ and $b_4 = d_3$. The divisors d_4, d_3 are coprime and so are b_3 and b_4. This is a contradiction since the system $\mathbf{S}$ is disjoint and so there are no coprime moduli. □

3. Existence of IDCS with Four Pairwise Distinct Moduli

Theorem 2.2 gives us one new necessary condition for moduli of non-natural IDCS . Now we shall show that the result of Theorem 2.2 is sharp.

Corollary 2.5 describes necessary condition for $\mu(\mathbf{S})$ where $\mathbf{S}$ is IDCS having exactly four moduli. The following theorem shows that this condition is sufficient.

Theorem 3.1. *Let $m = d_1d_2d_3d_4$ be a decomposition of m into product of four pairwise coprime numbers, where only d_4 may be equal to 1. Then there exists an irreducible disjoint covering system with the common modulus m and the set of moduli*

$$\mu(\mathbf{S}) = \{d_1d_2d_3, d_1d_2d_4, d_1d_3d_4, d_2d_3d_4\}\,.$$

Proof. Throughout the proof characters i, j, k, l are denoting one of the numbers 1, 2, 3, 4 (not necessary in this order) and are pairwise distinct. They are used as indices.

Denote

$$\mathbf{D}_i^+ = \{a;\ 0 \le a < d_i/2\}$$
$$\mathbf{D}_i^- = \{a;\ d_i/2 \le a < d_i\}\,.$$

$$\mathbf{S}_1 = \{a_1 \pmod{d_1} \cap a_2 \pmod{d_2} \cap a_4 \pmod{d_4};\ [a_1, a_2, a_4] \in \mathbf{D}_1^+ \times \mathbf{D}_2^- \times \mathbf{D}_4^+ \cup \mathbf{D}_1^- \times \mathbf{D}_2^+ \times \mathbf{D}_4^-\}$$
$$\mathbf{S}_2 = \{a_2 \pmod{d_2} \cap a_3 \pmod{d_3} \cap a_4 \pmod{d_4};\ [a_2, a_3, a_4] \in \mathbf{D}_2^+ \times \mathbf{D}_3^- \times \mathbf{D}_4^+ \cup \mathbf{D}_2^- \times \mathbf{D}_3^+ \times \mathbf{D}_4^-\}$$
$$\mathbf{S}_3 = \{a_3 \pmod{d_3} \cap a_1 \pmod{d_1} \cap a_4 \pmod{d_4};\ [a_3, a_1, a_4] \in \mathbf{D}_3^+ \times \mathbf{D}_1^- \times \mathbf{D}_4^+ \cup \mathbf{D}_3^- \times \mathbf{D}_1^+ \times \mathbf{D}_4^-\}$$
$$\mathbf{S}_4 = \{a_1 \pmod{d_1} \cap a_2 \pmod{d_2} \cap a_3 \pmod{d_3};\ [a_1, a_2, a_3] \in \mathbf{D}_1^+ \times \mathbf{D}_2^+ \times \mathbf{D}_3^+ \cup \mathbf{D}_1^- \times \mathbf{D}_2^- \times \mathbf{D}_3^-\}$$

$$\mathbf{S} = \mathbf{S}_1 \cup \mathbf{S}_2 \cup \mathbf{S}_3 \cup \mathbf{S}_4.$$

From assumption there follows that only $\mathbf{D}_4^-$ may be empty (that is true only if $d_4 = 1$) and so the sets $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{S}_4$ are nonvoid.

1. We shall prove that $\mathbf{S}$ is a covering system. Let z be any integer. Then there exist integers a_i $(1 \le i \le 4)$ such that

$$z \in a_1 \pmod{d_1} \cap a_2 \pmod{d_2} \cap a_3 \pmod{d_3} \cap a_4 \pmod{d_4}.$$

If $[a_1, a_2, a_3] \in \mathbf{D}_1^+ \times \mathbf{D}_2^+ \times \mathbf{D}_3^+ \cup \mathbf{D}_1^- \times \mathbf{D}_2^- \times \mathbf{D}_3^-$ then z is covered by $\mathbf{S}$.

Else there are two cases :

If $d_4 \in \mathbf{D}_4^+$ then one of the following conditions

$$a_1 \in \mathbf{D}_1^+ \ \&\ a_2 \in \mathbf{D}_2^- \text{ or } a_2 \in \mathbf{D}_2^+ \ \&\ a_3 \in \mathbf{D}_3^- \text{ or } a_3 \in \mathbf{D}_3^+ \ \&\ a_1 \in \mathbf{D}_1^-$$

is fulfilled and so z is covered by some $\mathbf{S}_i$ $(1 \le i \le 3)$. The case $d_4 \in \mathbf{D}_4^-$ can be proved similarly.

2. $\mathbf{S}$ is disjoint. It is enough to prove this property for each union $\mathbf{S}_i \cup \mathbf{S}_j$. From definition there follows that $\mathbf{S}_i$ $(1 \le i \le 4)$ is disjoint. So it is enough to prove that

$$b \,(\mathrm{mod}\ n) \cap b' \,(\mathrm{mod}\ n') = \emptyset \tag{3}$$

for $b \,(\mathrm{mod}\ n) \in \mathbf{S}_i$ and $b' \,(\mathrm{mod}\ n') \in \mathbf{S}_j$.

Let e.g. $i = 1$ and $j = 2$. From definition of $\mathbf{S}_1$ and $\mathbf{S}_2$ there follows that there are residue classes $a_4 \,(\mathrm{mod}\ d_4) \supseteq b \,(\mathrm{mod}\ n)$ and $a_4' \,(\mathrm{mod}\ d_4) \supset b' \,(\mathrm{mod}\ n')$. If $a_4 \neq a_4'$ then (3) holds. Else there are classes $a_2 \,(\mathrm{mod}\ d_2) \supseteq b \,(\mathrm{mod}\ n)$ and $a_2' \,(\mathrm{mod}\ d_2') \supseteq b' \,(\mathrm{mod}\ n')$. But a_2 and a_2' do not belong to the same set (one of them belong to $\mathbf{D}_2^+$ the other to $\mathbf{D}_2^-$) and so (3) holds. The remaining cases are similar.

Now it is sufficient to prove that $\mathbf{S}$ is irreducible. We shall proceed indirectly. Let $\mathbf{T}$ be a proper subsystem of $\mathbf{S}$ with at least two elements such, that the union of it's residue classes is a residue class:

$$\bigcup \left(a \,(\mathrm{mod}\ n);\ a \,(\mathrm{mod}\ n) \in \mathbf{T}\right) = e \,(\mathrm{mod}\ f). \tag{4}$$

The class $e \,(\mathrm{mod}\ f)$ contains all classes of the system $\mathbf{T}$, so f is a divisor of all moduli $n \in \mu(\mathbf{T})$ hence f divides their greatest common divisor.

The set of moduli $\mu(\mathbf{T})$ cannot contain all 4 moduli of $\mathbf{S}$ since their gratest common divisor is 1.

It cannot contain 3 moduli too since the greatest common divisor of any 3 moduli of $\mathbf{S}$ is one of the numbers d_i (still $1 \le i \le 4$). But if $d_i \neq 1$ then the system $\mathbf{S}$ contains a residue class $a \,(\mathrm{mod}\ n)$ with the modulus coprime to d_i and so coprime to f. Then

$$a \,(\mathrm{mod}\ n) \cap e \,(\mathrm{mod}\ f) \neq \emptyset \ \ \& \ \ a \,(\mathrm{mod}\ n) \nsubseteq e \,(\mathrm{mod}\ f),$$

what is a contradiction.

Let $\mu(\mathbf{T})$ contain 2 distinct moduli e.g. $d_i d_j d_k$ and $d_i d_j d_l$. Then f divides $d_i d_j$, so $e \,(\mathrm{mod}\ d_i d_j) \subseteq e \,(\mathrm{mod}\ f)$. Hence $e \,(\mathrm{mod}\ d_i d_j)$ has a nonvoid intersection only with some of the classes from $\mathbf{T}$. But every class from $\mathbf{T}$ is either subset of $e \,(\mathrm{mod}\ d_i d_j)$ or is disjoint with this class.

So there must be a subsystem $\mathbf{T'}$ of $\mathbf{T}$ such that

$$\bigcup \left(a \,(\mathrm{mod}\ n);\ a \,(\mathrm{mod}\ n) \in \mathbf{T'}\right) = e \,(\mathrm{mod}\ d_i d_j).$$

Let $\mathbf{T'}$ contain classes $b \,(\mathrm{mod}\ d_i d_j d_k)$ and $c \,(\mathrm{mod}\ d_i d_j d_l)$. The numbers b, c belong to $e \,(\mathrm{mod}\ d_i d_j)$ what implies that $d_i d_j = \gcd(d_i d_j d_k, d_i d_j d_l)$ divides $b - c$, what contradicts the disjointness of $\mathbf{S}$. Hence all classes in $\mathbf{T'}$ must have equal moduli.

We have shown, that if $\mathbf{S}$ contains proper subsystem $\mathbf{T}$ satisfying (4) then it contains proper subsystem $\mathbf{T'}$ ($\operatorname{card}(\mathbf{T'}) \geq 2$) having all residue classes with equal moduli.

It remains to prove that the system $\mathbf{S}$ cannot contain a proper subsystem $\mathbf{T}$ ($\operatorname{card}(\mathbf{T}) \geq 2$ containing classes with equal moduli.

Again by contradiction. Let all of the residue classes of $\mathbf{T}$ have the same modulus $d_i d_j d_k$. Then there is a prime p such that $f \mid (d_i d_j d_k/p)$ (since $f \mid d_i d_j d_k$ and $f \neq d_i d_j d_k$). Denote $f' = d_i d_j d_k/p$. The class $e \,(\operatorname{mod} f')$ is union of a subsystem $\mathbf{T'}$ of the system $\mathbf{T}$, where $\mathbf{T'}$ has exactly p residue classes. The prime p divides one of the numbers d_i, d_j, d_k. Let e.g. p divide d_i. Then there are residue classes $a_i \,(\operatorname{mod} d_i/p)$, $a_j \,(\operatorname{mod} d_j)$, $a_k \,(\operatorname{mod} d_k)$ such that

$$e \,(\operatorname{mod} f') = a_i \,(\operatorname{mod} d_i/p) \cap a_j \,(\operatorname{mod} d_j) \cap a_k \,(\operatorname{mod} d_k),$$

where $0 \leq a_i < d_i/p$, $0 \leq a_j < d_j$, $0 \leq a_k < d_k$.

Then every class $b_r \,(\operatorname{mod} m)$ of $\mathbf{T'}$ is of the form

$$b_r \,(\operatorname{mod} m) = (a_i + r d_i/p) \,(\operatorname{mod} d_i) \cap a_j \,(\operatorname{mod} d_j) \cap a_k \,(\operatorname{mod} d_k),$$

where $0 \leq r \leq p-1$. The second and the third class of the last intersection is the same for all the classes of $\mathbf{T'}$ and so by definition of the system $\mathbf{S}$ all the numbers $a_i + r d_i/p$ are elemetns of $\mathbf{D}_i^+$ or all of them are elements of $\mathbf{D}_i^-$. But $a_i < d_i/p \leq d_i/2$ what implies that a_i belongs to $\mathbf{D}_i^+$. On the other hand $a_i + (p-1)d_i/p \geq d_i/2$ what implies that $a_i + (p-1)d_i/p$ belongs to $\mathbf{D}_i^-$, what is contradiction. □

Remark 3.6. In [**3**] Korec proved that for the common modulus m there exists a non-natural IDCS if and only if m has at least three distinct prime divisors. Now this result is an immediate corollary of Theorems 2.2 and 3.1. Theorem 3.1 gives the direct construction of IDCS with the common modulus m.

H. Keller and G. Wirsching in [**1**] partially solved the problem: for which naturals m there is IDCS $\mathbf{S}$ with common modulus m such that there is no residue class $a \,(\operatorname{mod} m) \in \mathbf{S}$ (so called IDCS without supremum). The more general answer to their problem is given by Theorems 2.2 and 3.1:

Corollary 3.7. *Let m be a natural divisible by at least 4 distinct primes. Then there exists a non-natural* IDCS $\mathbf{S}$ *with common modulus m without supremum (there is no residue class $a \,(\operatorname{mod} m) \in \mathbf{S}$).*

Acknowledgement. The author wishes to thank to prof. Znám and doc. Korec for many valuable comments and suggestions.

References

1. Kellerer H. and Wirsching G., *Prime covers and periodic patterns*, Discrete Mathematics **85** (1990), 191–206.
2. Korec I., *Irreducible disjoint covering systems*, Acta Arithmetica **XLIV** (1984), 389–395.
3. ______, *Irreducible disjoint covering systems of* **Z** *with the common modulus consisting of three primes*, Acta Mathematica Universitatis Comenianae **XLVI–XLVII** (1985), 75–81.
4. Porubský Š., *Results and problems on covering systems of residue classes*, Mitt. Math. Semin. Giessen **150** (1982).
5. ______, *Natural exactly covering systems of congruences*, Czechoslovak Math. J. **26**(101) (1976), 145–153.
6. Znám Š., *A survey of covering systems of congruences*, Acta Mathematica Universitatis Comenianae **XL–XLI** (1982), 59–79.

I. Polách, Department of Algebra and Number Theory, Faculty of Mathematics and Physics, Comenius University, 842 15 Bratislava, Slovakia