UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
XLVI—XLVII—1985

IRREDUCIBLE DISJOINT CONVERING SYSTEMS OF Z WITH THE COMMON MODULUS CONSISTING OF THREE PRIMES

IVAN KOREC, Bratislava

Abstract. A disjoint covering system X consisting of k congruence classes (1.1) is said to be irreducible if the union of any of its r members, $1<r<k$, is not a congruence class. The least common multiple of its moduli $n_1, \ldots, n_k$ will be called the common modulus of X. The irreducible disjoint covering systems with the common modulus pqr where $p<q<r$ are primes, are described. It is proved that there are $(2^p-2)\cdot(2^q-2)\cdot(2^r-2)$ of them. Further, the bounds for $Ab_M(X)= k-(p+q+r-2)$ and for the number h_X of the elements of X with the modulus pqr are given by the formulae (2.4), (2.5).

1. Introduction and basic notions

The symbol Z will denote the set of integers. For integers $n>0$, a the symbol $a(\text{mod } n)$ will denote the congruence class $\{a+nx, x \in \mathrm{Z}\}$. The greatest common divisor of x, y will be denoted by $\mathrm{D}(x, y)$.

The intresection of any two congruence classes $\mathrm{X}=a(\text{mod } m)$, $\mathrm{Y}=b(\text{mod } n)$ is either empty or a congruence class. If m, n are relatively prime then the first case never takes place, and every congruence class modulo mn can be represented in the form $a(\text{mod } m)\cap b(\text{mod } n)$. Analogously, if p, q, r are relatively prime (and so more when they are different primes) every congruence class modulo pqr can be represented in the form

$$a(\text{mod } p)\cap b(\text{mod } q)\cap c(\text{mod } r)\,.$$

The system

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

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 they are given in (1.1) without repretition. The integers $n_1, \ldots, n_k$ will be called moduli of (1.1) and their least common multiple will be called the common modulus of (1.1).

The above mentioned property of congruence classes implies

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

A DCS (1.1) will be called irreducible disjoint covering system (abbreviated: IDCS) if $k > 1$ and there is no $M \subseteq \{1, \ldots, k\}$, $1 < \operatorname{card}(M) < k$ such that $\bigcup\{a_i (\bmod\, n_i);\, i \in M\}$ is a congruence class. Every DCS can be obtained from the trivial DCS $\{Z\}$ and several IDCS by the operation of splitting which is defined in [3]. Hence some problems concerning general DCS can be reduced to the same problems for IDCS. If p is a prime then the partition of Z into p congruence classes modulo p is an IDCS. For all other IDCS their moduli are relatively prime (but by (1.2) they cannot be pairwise relatively prime).

The example of so called non-natural DCS given by Š. Porubský [6] leads to an IDCS with the common modulus 30. Other examples are given in [3] where it is also shown that an IDCS with the common modulus m exists if and only if m is a prime or m is divisible by at least three different primes. In the next section we shall deal with the simplest possibility when m is the product of three different primes p, q, r, and we shall describe all IDCS with the common modulus of this form.

Let us define $\mathscr{F}(p) = p - 1$ for every prime p, and extend the function $\mathscr{F}$ to the set of all positive integers by the formula $\mathscr{F}(m \cdot n) = \mathscr{F}(m) + \mathscr{F}(n)$. Further, if X is the DCS (1.1), let us call the number

$$\mathrm{Ab}_M(X) = k - (1 + \max(\mathscr{F}(n_1), \mathscr{F}(n_2), \ldots, \mathscr{F}(n_k)) \tag{1.3}$$

the Mycielski's abundance of X. The hypothesis formulated by Mycielski and Sierpinski in [5] which is proved by Znám in [8] states

$$\mathrm{Ab}_M(X) \geqq 0 \tag{1.4}$$

for every DCS X.

For every IDCS whose common modulus is a prime the equality in (1.4) holds. For all other IDCS the inequality $\mathrm{Ab}_M(X) \geqq 5$ is proved in [4]. (Notice that (1.4) holds also for DCS of arbitrary abelian groups but the last inequality does not.) In this paper the exact bounds for $\mathrm{Ab}_M(X)$ are given provided that the common modulus of DCS X is the product of three primes.

2. Results on irreducible disjoint covering systems

Theorem 1. Let p, q, r be pairwise different primes. Then for every IDCS X with the common modulus pqr there are sets P_q, P_r, Q_p, Q_r, R_p, R_q such that:

(i) $\{P_q, P_r\}$, $\{Q_p, Q_r\}$, $\{R_p, R_q\}$ are partitions of the sets $P=\{0, 1, \ldots, p-1\}$, $Q=\{0, 1, \ldots, q-1\}$, $R=\{0, 1, \ldots, r-1\}$, respectively.

(ii) For every $a \in P$, $b \in Q$ it holds

$$a(\text{mod } p) \cap b(\text{mod } q) \in \mathrm{X} \text{ if and only if } a \in P_q \text{ and } b \in Q_p\,; \tag{2.1}$$

analogously for the moduli pr, qr instead of pq.

(iii) For every $a \in P$, $b \in Q$, $c \in R$ it holds

$$a(\text{mod } p) \cap b(\text{mod } q) \cap c(\text{mod } r) \in \mathrm{X} \tag{2.2}$$

if and only if

$$(a \in P_q \text{ and } b \in Q_r \text{ and } c \in R_p) \text{ or } (a \in P_r \text{ and } b \in Q_p \text{ and } c \in R_q)\,. \tag{2.3}$$

Conversely, to every ordered sixtuple of sets P_q, P_r, Q_p, Q_r, R_p, R_q which satisfies (i) there is exactly one IDCS X with the common modulus pqr such that (ii), (iii) hold.

Proof. Let X be an IDCS with the common modulus pqr. Then its moduli can be only pqr, pq, pr, qr; the other divisors of pqr are excluded by (1.2). Define

$$P_q=\{a \in \mathrm{P}; (\exists b \in \mathrm{Q})\, (a(\text{mod } p) \cap b(\text{mod } q) \in \mathrm{X}\}$$
$$P_r=\{a \in \mathrm{P}; (\exists c \in \mathrm{R})\, (a(\text{mod } p) \cap c(\text{mod } r) \in \mathrm{X}\}$$
$$Q_p=\{b \in \mathrm{Q}; (\exists a \in \mathrm{P})\, (a(\text{mod } p) \cap b(\text{mod } q) \in \mathrm{X}\}$$

and analagously defines Q_r, R_p, R_q. (The notation used allows the permutation (PQR) (pqr) (abc) of the letters.)

If $P_q \cap P_r \neq \emptyset$ then there are $a \in P_q \cap P_r$, $b \in Q$ and $c \in R$ such that

$$a(\text{mod } p) \cap b(\text{mod } q) \in \mathrm{X} \text{ and } a(\text{mod } p) \cap c(\text{mod } r) \in \mathrm{X}$$

Since these elements of X are different we have

$$a(\text{mod } p) \cap b(\text{mod } q) \cap c(\text{mod } r)=\emptyset$$

which is a contradiction. Therefore $P_q \cap P_r=\emptyset$, and analogously $Q_p \cap Q_r=\emptyset$, $R_p \cap R_q=\emptyset$.

If $P_q=\emptyset$ then X does not contain any element with the modulus pq. Hence all moduli of X are multiples of r, which is a contradiction. Therefore $P_q \neq \emptyset$, and analogously the other sets P_r, Q_p, Q_r, R_p, R_q are nonempty.

To prove $P_q \cup P_r=P$ consider $a \in P-P_r$; we shall prove $a \in P_q$. Since P_q is nonempty there are $a_1 \in P_q$, $b \in Q$ such that $\mathrm{Y}_1=a_1(\text{mod } p) \cap b(\text{mod } q) \in \mathrm{X}$. We shall prove that $Y = a(\text{mod } p) \cap b(\text{mod } q)$ belongs to X, too. Since $a \in P - P_r$ the set X does not contain $a(\text{mod } p) \cap c(\text{mod } r)$ for any $c \in R$. Further, the set X cannot contain any element of the form $b(\text{mod } q) \cap c(\text{mod } r)$ because it has nonempty intersection with Y_1. Therefore Y is the union of a subset of X, and since X is irreducible we have $Y \in X$, and hence $a \in P_q$. Hence $\{P_q, P_r\}$ is a partition of P, and analogously $\{Q_p, Q_r\}$ is a partition of Q, and $\{R_p, R_q\}$ is a partition of R.

Now we shall prove (ii). The direct implication is obvious. Conversely, let $a \in P_q$ and $b \in Q_p$. Then there is $a_1 \in P$ such that $Y_1 = a_1(\text{mod } p) \cap b(\text{mod } q) \in X$. Since $a \in P - P_r$, we can obtain $a(\text{mod } p) \cap b(\text{mod } q) \in X$ in the same way as above.

To prove (iii) assume (2.2) at first. Then $a(\text{mod } p) \cap b(\text{mod } q) \neq X$, and hence $a \in P_r$ or $b \in P_r$. Analogously $a \in P_q$ or $c \in R_q$, and also $b \in Q_p$ or $c \in R_p$. If $a \in P_q$ then $a \notin P_r$, and hence $b \in Q_r$. Therefore $b \notin Q_p$, and hence $b \in Q_r$. The case $a \in P_r$ is similar. Conversely, assume 2.3. If, for example,

$$a \in P_q \quad \text{and} \quad b \in Q_r \quad \text{and} \quad c \in R_p\,,$$

then $b \notin Q_p$, and hence $a(\text{mod } p) \cap b(\text{mod } q) \notin X$. Analogously $a(\text{mod } p) \cap c(\text{mod } r) \notin X$ and $b(\text{mod } q) \cap c(\text{mod } r) \notin X$, and hence (2.2) holds.

Now assume that the sets P_q, P_r, Q_p, Q_r, R_p, R_q satisfy (i). The conditions (ii), (iii) uniquely determine a set X of congruence classes with the moduli pq, pr, qr and pqr. We only have to prove that X is an IDCS. To prove that X is a DCS it suffices to realize that for every $a \in P$, $b \in Q$, $c \in R$ exactly one of the four conditions

$$a \in P_q \text{ and } b \in Q_p,\ a \in P_r \text{ and } c \in R_p,\ b \in Q_r \text{ and } c \in R_p\,,$$

and (2.3) is fulfilled. They determine the modulus (pq, pr, qr, or pqr, respectively) of the element of X which contains

$$a(\text{mod } p) \cap b(\text{mod } q) \cap c(\text{mod } r)\,.$$

It remains to show that the DCS X is irreducible. If not, then there is a proper subset Y of X, $\text{card}(Y) \geqq 2$, such that $\bigcup Y$ is a congruence class with a modulus m. Obviously $1 < m < pqr$ and m divides pqr. However, $m \neq p$ because X contains an element with the modulus qr (see (1.2)); analogously $m \neq q$, $m \neq r$. Hence $m \in \{pq, pr, qr\}$; let e.g. $m = pq$. Then there are $a \in P$, $b \in Q$ such that for every $c \in R$ (2.2) holds, and hence (2.3) holds, too. Considering $c \in R_p$ (i.e. $c \notin R_q$) we obtain $a \in P_q$ and considering $c \in R_q$ we obtain $a \in P_r$. Therefore $P_r \cap P_q = \emptyset$, which is a contradiction.

Corollary 1. If p, q, r are pairwise different primes then there are exactly $(2^p - 2) \cdot (2^q - 2) \cdot (2^r - 2)$ irreducible DCS with the common modulus pqr.

Proof. Every IDCS X with the common modulus pqr is determined by an ordered triple (P_q, Q_r, R_p) of proper subsets of P, Q, R, and there are $2^p - 2$, $2^q - 2$, $2^r - 2$ possibilities for P_q, Q_r, R_p, respectively.

Remark. It seems reasonable to classify IDCS from Theorem 1 by the cardinalities of the sets P_q, Q_p, Q_p, Q_r, R_p, R_q (or, equivalently, by the primes p, q, r and the cardinalities of P_q, Q_r, R_p).

Theorem 2. If X is an IDCS with the common modulus pqr, where $p<q<r$ are primes, then

$$(p-1)\cdot(q+r-3)\leqq \mathrm{Ab}_{\mathrm{M}}(\mathrm{X})\leqq (p-1)\cdot(q-1)\cdot(r-1)\,. \tag{2.4}$$

Further, if $\mathrm{h_X}$ is the number of elements of X with the modulus pqr then

$$(p-1)\cdot(q-1)+(r-1)\leqq \mathrm{h_X}\leqq (p-1)\cdot(q-1)\cdot(r-1)+1\,. \tag{2.5}$$

The bounds in (2.4), (2.5) are the best possible.

Proof. Let P_q, Q_r, R_p be the sets coordinated to X in Theorem 1, and let x, y, z be their cardinalities, respectively. Then $a(\mathrm{mod}\ p)\cap b(\mathrm{mod}\ q)\in \mathrm{X}$ if and only if $a\in P_q$ and $b\notin Q_r$, hence X contains $x\cdot(q-y)$ elements with the modulus pq; analogously we can determine the number of elements of X which have moduli pq and qr. By the condition (iii) of Theorem 1 X contains $xyz+(p-x)\cdot(p-y)\cdot(p-z)$ elements with the modulus pqr. Hence X consists of

$$f(x,y,z)=xyz+(p-x)\cdot(q-y)\cdot(r-z)+x\cdot(q-y)+y\cdot(r-z)+z\cdot(p-x)$$

congruence classes. To obtain (2.4) we have to determine the extrems of the function f for

$$1\leqq x\leqq p-1,\quad 1\leqq y\leqq q-1,\quad 1\leqq z\leqq r-1\,. \tag{2.6}$$

If x, y are fixed then $g(z)=f(x,y,z)$ is a linear function of z. Hence it reaches its extrems for $z=1$, $z=r-1$ (or $g(z)$ is a constant function, and the choice of z is inessential). Therefore it suffices to consider $z\in\{1,r-1\}$, and analogously $x\in\{1,p-1\}$, $y\in\{1,q-1\}$. To make the formulae below shorter, denote $a=p-1$, $b=q-1$, $c=r-1$. By an easy computation we obtain

$$\begin{aligned}
&f(1,1,1)=f(a,b,c)=1+abc+a+b+c\\
&f(1,1,c)=f(a,1,c)=c+ab+b+1+ac=(a+1)(b+c)+1\\
&f(1,b,1)=f(1,b,c)=b+ac+1+bc+a=(c+1)(a+b)+1\\
&f(a,1,1)=f(a,b,1)=a+bc+ab+c+1=(b+1)(a+c)+1
\end{aligned}$$

Since $1\leqq a<b<c$ we can easily obtain

$$f(1,1,c)<f(a,1,1)\leqq f(1,b,1)\leqq f(1,1,1)\,.$$

Therefore

$$f(1,1,c)\leqq \mathrm{card}(\mathrm{X})\leqq f(1,1,1)\,.$$

Since $\mathrm{Ab}_{\mathrm{M}}(\mathrm{X})=\mathrm{card}(\mathrm{X})-(\mathscr{F}(pqr)+1)=\mathrm{card}(\mathrm{X})-(a+b+c+1)$ we have

$$f(1, 1, c)-(a+b+c+1) \leqq \mathrm{Ab_M}(\mathrm{X}) \leqq f(1, 1, 1)-(a+b+c+1)$$
$$a \cdot (b+c-1) \leqq \mathrm{Ab_M}(\mathrm{X}) \leqq abc$$

which is (2.4).

To prove (2.5), consider analogously the function

$$h(x, y, z)=xyz+(p-x) \cdot (p-y) \cdot (p-z)$$

for x, y, z satisfying (2.6). We can easily obtain

$$h(1, 1, c) \leqq h(x, y, z) \leqq h(1, 1, 1)$$

which immediately gives (2.5).

Corollary 2. For every integer n_0 there are only finitely many IDCS X such that their common moduli are product of three primes and $\mathrm{Ab_M}(\mathrm{X}) \leqq n_0$.

Remark. Generally speaking, the common modulus m of a DCS X need not occur among its moduli (see [1]). However, by (2.5) m occurs among them for IDCS X from the above theorems. Therefore (2.4) holds also for the so-called Mycielski—Znám's abundance which is defined by the formula

$$\mathrm{Ab_{MZ}}(\mathrm{X})=k-(1+\mathscr{F}(m)) .$$

REFERENCES

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

[2] Friedlander, J.: On exact covering of the integers, Israel J. Math. 12 (1972) 299—305.

[3] Korec, I.: Irreducible disjoint covering systems. Acta Arithmetica. XLN (1984), 389—395.

[4] Korec, I.: Improvement of Mycielski's inequality for nonnatural disjoint covering systems of Z. To appear.

[5] Mycielski, J.—Sierpiński, W.: Sur une propriété des ensembles linéaires, Fund. Math. 58(1966), 143—147.

[6] Porubský, Š.: Natural exactly covering systems of congruences, Czech. Mat. Journal 24 (1974), 598—606.

[7] Porubský, Š.: Results and problems on covering systems of residue classes, Mitt. Math. Semin. Giessen, Heft 150, 1981, 1—85.

[8] Znám, Š.: On Mycielski's problem on systems of arithmetical progressions, Coll. Math. 15 (1966), 201—204.

[9] Znám, Š.: A survey of covering systems of congruences, Acta Math. Univ. Comen. 40—41 (1982), 59—79.

Author's address:
Ivan Korec
Katedra algebry a teórie čísel MFF UK
Mlynská dolina
842 15 Bratislava

Received: 19. 1. 1984

РЕЗЮМЕ

НЕРАЗЛОЖИМЫЕ ТОЧНО НАКРЫВАЮЩИЕ СИСТЕМЫ ЦЕЛИХ ЧИСЕЛ С ОБЩИМ МОДУЛЕМ СОСТОЯЩИМ ИЗ ТРЕХ ПРОСТЫХ ЧИСЕЛ

Иван Корец, Братислава

Точно накрывающая система X состоящая из смежных классов (1.1) будет называться неразложимой если ни для каких r классов из X, $1<r<k$, объединение не является смежным классом. Наименьшее общее кратное модулей $n_1, \ldots, n_k$ будет называться общим модулем системы X. Доказывается, что если $p<q<r$ простые числа то существует точно $(2^p-2)\cdot(2^q-2)\cdot(2^r-2)$ неразложимых точно накрывающих систем с общим модулем pqr. Далее получаются оценки (2.4), (2.5) для числа $\mathrm{Ab}_M(X)=k-(p+q+r-2)$ и для числа h_X элементов X с общим модулем pqr.

SÚHRN

IREDUCIBILNÉ PRESNE POKRÝVAJÚCE SÚSTAVY NA Z, KTORÝCH MODUL JE SÚČINOM TROCH PRVOČÍSEL

Ivan Korec, Bratislava

Presne pokrývajúcu sústavu X, pozostávajúcu z k zvyškových tried (1.1) budeme nazývať ireducibilnou, ak zjednotenie žiadnych r jej prvkov, $1<r<k$, nie je zvyšková trieda. Najmenší spoločný násobok jej modulov $n_1, \ldots, n_k$ budeme nazývať jej spoločným modulom. Vyšetrujú sa ireducibilné presne pokrývajúce sústavy, ktorých spoločný modul je súčinom troch prvočísel p, q, r. Dokazuje sa, že existuje presne $(2^p-2)\cdot(2^q-2)\cdot(2^r-2)$ takýchto sústav. Ďalej sú nájdené presné dolné a horné odhady (2.4) a (2.5) pre číslo $\mathrm{Ab}_M(X)=k-(p+q+r-2)$ a pre počet h_X prvkov X, ktorých modul je pqr.