Mathematica Slovaca

Štefan Porubský; Johanan Schönheim

Old and new necessary and sufficient conditions on (a_i, m_i) in order that $n \equiv a_i (\mathrm{mod}\, m_i)$ be a covering system

Mathematica Slovaca, Vol. 53 (2003), No. 4, 341--349

Persistent URL: http://dml.cz/dmlcz/132814

Mathematica Slovaca
© 2003
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **53** (2003), No. 4, 341–349

OLD AND NEW NECESSARY AND SUFFICIENT CONDITIONS ON (a_i, m_i) IN ORDER THAT $n \equiv a_i \pmod{m_i}$ BE A COVERING SYSTEM

ŠTEFAN PORUBSKÝ* — JOCHANAN SCHÖNHEIM**

(*Communicated by Stanislav Jakubec*)

ABSTRACT. A covering system is a set of congruences $n \equiv a_i \pmod{m_i}$, $i = 1, \dots k$, such that every integer satisfies at least one of them. A new necessary and sufficient condition in order that a given set of congruences $n \equiv a_i \pmod{m_i}$ be a covering system is established and its correlations to known conditions are studied.

Let

$$n \equiv a_i \pmod{m_i}\,, \quad i = 1, 2, \dots, k\,, \tag{1}$$

be a system of congruence classes. We shall always suppose that the offsets of congruences in (1) are *standardized*, that is that $0 \leq a_i < m_i$ for every $i \in \{1, 2, \dots, k\}$, and use the shorthand notation $(a_i, m_i)_{i=1}^{k}$ for (1).

The *covering function* of (1) is defined through (cf. [4])

$$\mathfrak{m}(n) = \sum_{i=1}^{k} \left[n \equiv a_i \pmod{m_i}\right], \qquad n \in \mathbb{Z}\,,$$

where the Iverson's brackets notation $\left[n \equiv a \pmod{b}\right]$ stands for the indicator of the class $a \pmod{b}$. The function $\mathfrak{m}$ is obviously periodic and its (least nonnegative) period will be denoted by m_0. The period m_0 always divides the number $m = \text{l. c. m.}[m_1, m_2, \dots, m_k]$. In Table 1 one of the possible schemes for determination of the covering function of system

$$0 \pmod 2\,,\ 0 \pmod 3\,,\ 1 \pmod 4\,,\ 1 \pmod 6\,,\ 11 \pmod{12} \tag{2}$$

2000 Mathematics Subject Classification: Primary 11B25, 11B68.
Keywords: arithmetic sequence, covering system, exactly covering system, disjoint covering system.

The first author was supported by the Grant Agency of the Czech Republic, Grant # 201/01/0471.

is given. In the table the head row contains the complete set of residues modulo m_0, the period of its covering function. Each middle row shows whether or not the residue at the top of the column belongs to the class given at the head of the row.

TABLE 1.
COVERING FUNCTION OF (2).

	0	1	2	3	4	5	6	7	8	9	10	11
(0,2)	|		|		|		|		|		|	
(0,3)	|			|		|			|			
(1,4)		|				|				|			
(1,6)		|						|					
(11,12)														|
m	2	2	1	1	1	1	2	1	1	2	1	1

The covering function and its properties can be used for various classifying systems (1). If

(a) $\mathrm{m}(n) \geq 1$ for every $n \in \mathbb{Z}$, then we say that (1) is a *covering system.* This is the class of systems (1) Paul Erdős had in mind when he introduced the concept. System (2) is covering with the least possible k when the moduli are distinct;
(b) $\mathrm{m}(n) \leq 1$ for every $n \in \mathbb{Z}$, then we say that (1) is a *disjoint system*;
(c) $\mathrm{m}(n) = 1$ for every $n \in \mathbb{Z}$, then we say that (1) is an *exact covering system.*

If we replace number 1 by a general positive integer M, we get further notions: If

(d) $\mathrm{m}(n) \geq M$ for every $n \in \mathbb{Z}$, then we say that (1) is an M *covering system*;
(e) $\mathrm{m}(n) \leq M$ for every $n \in \mathbb{Z}$, then we say that (1) is an *at most* M *covering system*;
(f) $\mathrm{m}(n) = M$ for every $n \in \mathbb{Z}$, then we say that (1) is an *exact* M *covering system.*

There are also classification criteria based on properties of the involved congruence classes. Let us mention two of them (the reader is referred to [7] for other possibilities):

(g) A congruence of the system (1) is called *essential* if there exists an integer which satisfies this and only this congruence. System (1) is called *regular* or *irredundant* if all its classes are essential.
(h) System (1) is called *incongruent* if all its moduli are distinct.

Following [9], given a system (1), we assign it the additive group

$$G = G(m_1, \ldots, m_k) = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}\,, \tag{3}$$

which is the Cartesian product of additive groups of the complete residue system modulo each modulus of (1). Denote by H its subgroup generated by the k-tuple $\mathbf{h} = (1, 1, \ldots, 1)$. The order of G is $m_1 m_2 \cdots m_k$, while the order of H is l. c. m.$[m_1, m_2, \ldots, m_k]$.

TABLE 2.
THE COSET GENERATED BY THE OFFSETS OF (2).

n	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z}$	# of 0's
0	0	0	1	1	11	2
1	1	1	2	2	0	1
2	0	2	3	3	1	1
3	1	0	0	4	2	2
4	0	1	1	5	3	1
5	1	2	2	0	4	1
6	0	0	3	1	5	2
7	1	1	0	2	6	1
8	0	2	1	3	7	1
9	1	0	2	4	8	1
10	0	1	3	5	9	1
11	1	2	0	0	10	2

The coset generated in G by H and containing the offsets of (2) is given in Table 2. Here the first column indicates the multiple of $\mathbf{h}$ which is added to the original set of offsets. All the elements are standardized modulo the corresponding modulus. In [9] a coset C was defined as *good* if each element of C has at least one zero component. The last column of the table gives the number of zero components in the corresponding coset element, confirming again the fact that (2) is covering.

Now we can modify the Table 1 as follows: On every place where the indicators stand we write zero and continue with filling in the row with shifted standardized offsets modulo the corresponding modulus of the class in the head of the row as shown in Table 3. The last row gives the number of zeros in the column. Clearly this row coincides with that of Table 1, but differs from the corresponding last column in Table 2.

TABLE 3.

	0	1	2	3	4	5	6	7	8	9	10	11
(0,2)	0	1	0	1	0	1	0	1	0	1	0	1
(0,3)	0	1	2	0	1	2	0	1	2	0	1	2
(1,4)	3	0	1	2	3	0	1	2	3	0	1	2
(1,6)	5	0	1	2	3	4	5	0	1	2	3	4
(11,12)	1	2	3	4	5	6	7	8	9	10	11	0
# of 0's	2	2	1	1	1	1	2	1	1	2	1	1

To see the reason for this difference, note that the main mechanism behind the construction of Table 2 is the function

$$T_i^+(n) = n + a_i \pmod{m_i}$$

applied to the ith column, $i = 1, 2, \ldots, k$. In Table 3 the same role plays the function

$$T_i^-(n) = n - a_i \pmod{m_i}$$

applied to the ith row. Thus starting with the system $(-a_i, m_i)_{i=1}^k$ in Table 3 we get Table 2 as demonstrated in Table 4 using our selected sample system (2).

TABLE 4.

	0	1	2	3	4	5	6	7	8	9	10	11
(0,2)	0	1	0	1	0	1	0	1	0	1	0	1
(0,3)	0	1	2	0	1	2	0	1	2	0	1	2
(3,4)	1	2	3	0	1	2	3	0	1	2	3	0
(5,6)	1	2	3	4	5	0	1	2	3	4	5	0
(1,12)	11	0	1	2	3	4	5	6	7	8	9	10
# of 0's	2	1	1	2	1	1	2	1	1	1	1	2

Given a coset C of H in G represented by k-tuple $(a_1, \ldots, a_k) \in G$, define the *zeros counting functions* $\mathfrak{z}(n)$ of C at $n \in \mathbb{Z}$ as the number of zero components of the element $(a_1, \ldots, a_k) + n\mathbf{h}$ of C. Since

$$\mathfrak{z}(n) = \sum_{i=1}^{k} [T_i^-(n) = 0],$$

the above ideas in their general form lead to:

THEOREM 1. *If C is a coset of H represented by $(-a_1, \ldots, -a_k) \in G$, then the zeros counting function $\mathfrak{z}(n)$ of C and the covering function $\mathfrak{m}(n)$ of* (1) *coincide for all $n \in \mathbb{Z}$.*

Given a system (1), the system $x \equiv -a_i \pmod{m_i}$ will be called the *conjugate* of (1). Thus the previous result can be expressed in the form:

The covering function of a system and the zeros counting function of its conjugate are the same.

When considering the zeros counting function, we actually considered only the following values of the argument $n = 0, 1, \ldots, m-1$. The zeros counting function can be in a natural way extended as a function of an arbitrary integer argument.

Two systems $(a_i, m_i)_{i=1}^{k}$, and $(b_j, n_j)_{j=1}^{s}$ will be called *covering similar* if their covering functions $\mathfrak{m}_1$, and $\mathfrak{m}_2$, resp. are shifted, i.e. there is an integer s such that

$$\mathfrak{m}_1(n) = \mathfrak{m}_2(n+s)$$

holds for every $n \in \mathbb{Z}$.

COROLLARY 1.1. *If $(a_i, \ldots, a_k)$ and $(b_i, \ldots, b_k)$ are elements of the same coset C modulo H, then the systems $n \equiv a_i \pmod{m_i}$ and $n \equiv b_i \pmod{m_i}$, $i = 1, \ldots, k$, are covering similar.*

Notice that, by the above results, all systems with a given set of moduli $m_1, m_2, \ldots, m_k$ and prescribed covering function can be given, if any, as the members of certain (possibly more) cosets.

For instance, if $m_1 = 3$, $m_2 = m_3 = 6$, and $m_4 = m_5 = m_6 = 9$, we have 78 732 various systems of congruence classes which split into 4 374 cosets modulo H. It is proved in [11] that with (1) also the system $m_i - a_i - 1 \pmod{m_i}$, $i = 1, \ldots, k$, is exact covering. Thus, for instance, both systems

$$0 \pmod 3,\ 1 \pmod 6,\ 4 \pmod 6,\ 2 \pmod 9,\ 5 \pmod 9,\ 8 \pmod 9$$

and

$$2 \pmod 3,\ 4 \pmod 6,\ 1 \pmod 6,\ 6 \pmod 9,\ 3 \pmod 9,\ 0 \pmod 9$$

are exact covering, and therefore covering similar. However, the sixtuples of their offsets belong to different cosets modulo H. This shows that the last Corollary cannot be reversed.

This gives another proof of the following result:

COROLLARY 1.2. ([9; Theorem 1]) *A set of positive integers $0 < m_1 \leq m_2 \leq \cdots \leq m_k$ can serve as a set of moduli of a covering system if and only if among the cosets of H in $G = G(m_1, \ldots, m_k)$ there is a good one.*

Moreover, if $(a_1, \ldots, a_k)$ is an arbitrary element of a good coset, then

$$n \equiv -a_i \pmod{m_i}, \qquad i = 1, \ldots, k, \tag{4}$$

is a covering system. Conversely, if (4) *is a covering system, then the coset represented by* $(a_1, \ldots, a_k)$ *is good.*

The coset H has a special position, it is *never good*. It can be used to generalize the Chinese Remainder Theorem. Namely, $(a_1, a_2, \ldots, a_k) \in H$ if and only if the system (1) has a solution. We believe also that the members of H answer the question which has been raised, namely, for what $(a_1, a_2, \ldots, a_k)$ system (1) is the worst one, that is one which leaves "most" integers uncovered.

Theorem 1 enables us to rewrite the definitions depending on properties of covering function in terms of "number of zeros" of elements of sets, leading thus to a series of theorems having the spirit of Corollary 1.2. For instance:

> *A set of positive integers* $0 < m_1 \leq m_2 \leq \cdots \leq m_k$ *can serve as a set of moduli of an exact covering if and only if among the cosets of* H *in* $G = G(m_1, \ldots, m_k)$ *there is one in which each element has a unique vanishing component*, etc.

In 1973, A. S. Fraenkel discovered a characterization of exact covering systems in terms of Bernoulli polynomials. This result was later extended to various systems of congruences by Porubský [4], [5], [6], J. Beebee [1] and Z.-W. Sun [10]. For general systems (1) the following result was proved:

LEMMA 2. ([4; Theorem 2], [6; Theorem 1]) *Let* n *be any real number. Then a system* (1) *has covering function* $\mathfrak{m}$ *if and only if*

$$m_0^{r-1} \sum_{t=0}^{m_0-1} \mathfrak{m}(t) B_r\left(\frac{n+t}{m_0}\right) = \sum_{t=1}^{k} m_t^{r-1} B_r\left(\frac{n+a_t}{m_t}\right) \tag{5}$$

holds for every non-negative integer r.

For $r = 0$ and $r = 1$ we get from this result

$$\sum_{i=1}^{k} \frac{1}{m_i} = \frac{1}{m_0} \sum_{t=0}^{m_0-1} \mathfrak{m}(t) \tag{6}$$

and

$$\sum_{i=1}^{k} \frac{a_i + n}{m_i} = \frac{k}{2} + \sum_{t=0}^{m_0-1} \mathfrak{m}(t) \left(\frac{t+n}{m_0} - \frac{1}{2}\right). \tag{7}$$

Now we prove a result which we use to derive a new necessary and sufficient condition in order that a given set of congruences (1) be a covering system is established. We show that:

THEOREM 3. *If $\mathfrak{z}$ is the zeros counting function of a system* (1), *then*

$$\sum_{i=1}^{k} \frac{1}{m_i} - \sum_{i=1}^{k} \frac{a_i + n + 1}{m_i} + \sum_{i=1}^{k} \frac{a_i + n}{m_i} = \mathfrak{z}(n+1) \tag{8}$$

for every $n = 0, 1, \ldots, [m_1, \ldots, m_k] - 1$, where $a_i + n + 1$ and $a_i + n$ are always standardized modulo m_i, $i = 1, \ldots, k$.

P r o o f . The proof will be based on the relation

$$\sum_{i=1}^{k} \frac{a_i + n + 1}{m_i} - \sum_{i=1}^{k} \frac{a_i + n}{m_i} = \sum_{i=1}^{k} \frac{1}{m_i}, \tag{9}$$

which valid for any $n \in \mathbb{Z}$. Relation (9) can be verified immediately by a direct computation, or using (6) and (7). It is important to note that in (9) the numbers $a_i + n + 1$, and $a_i + n$ are not standardized modulo m_i, even if a_i are supposed to be.

To standardize the numerators, replace the numbers $a_i + n + 1$, and $a_i + n$ for every $i = 1, \ldots, k$ on left hand side of (9), by their least non-negative remainder. For those indices $i \in \{1, \ldots, k\}$ for which $m_i \nmid a_i + n + 1$ this can be done immediately, because for those a_i's the difference

$$\frac{a_i + n + 1}{m_i} - \frac{a_i + n}{m_i} \tag{10}$$

remains unchanged after substitution. Its value is $1/m_i$, as it can be easily seen. This means that for index i such that $m_i \nmid a_i + n + 1$, the value of the difference (10) on the left hand side of (9) cancels with that of $1/m_i$ in sum of reciprocals of moduli on the right hand side of (9).

On the other hand, for those i's for which $m_i \mid a_i + n + 1$, the difference (10) equals $(m_i - 1)/m_i$. Together with the corresponding term in the sum of reciprocals of moduli we get 1, as the final contribution of each such i. Therefore

$$\sum_{i=1}^{k} \frac{a_i + n + 1}{m_i} - \sum_{i=1}^{k} \frac{a_i + n}{m_i} = \sum_{i=1}^{k} \frac{1}{m_i} = \sum_{i=1}^{k} \left[n + 1 \equiv -a_i \pmod{m_i} \right].$$

The sum on the right is the covering function of the conjugate system to the original one evaluated at $n + 1$ and Theorem 1 finishes the proof. □

The following simple necessary and sufficient condition on (a_i, m_i) in order that (1) be a covering system can be readily derived from the previous result:

COROLLARY 3.1. *A system* (1) *is covering if and only if*

$$\sum_{i=1}^{k} \frac{1}{m_i} > \sum_{i=1}^{k} \frac{a_i + n + 1}{m_i} - \sum_{i=1}^{k} \frac{a_i + n}{m_i} \tag{11}$$

with the range of n *and the standardization as above.*

P r o o f . The necessity is immediate because then the covering system has positive both covering and zeros counting functions. To prove the sufficiency, note that difference in (10) changes only if $m_i \mid a_i + n + 1$. Since the corresponding change always decreases the value on the left hand side of (9), two or more such divisibility relations cannot compensate mutual changes. Thus if (11) holds, we must have at least one such divisibility relation, which means that, in Table 2, we have at least one zero in each row, i.e. our system (1) is covering. □

For exact M covering systems, where $\sum_{i=1}^{k} m_i^{-1} = M$ and $\mathfrak{m}(n) = M$ for every n, we get the following generalization of the third part of [8; Theorem 2]:

COROLLARY 3.2. *A system* (1) *is exact* M *covering if and only if*

$$\sum_{i=1}^{k} \frac{1}{m_i} = M \tag{12}$$

and

$$\sum_{i=1}^{k} \frac{a_i + 1 + n}{m_i} - \sum_{i=1}^{k} \frac{a_i + n}{m_i} = 0 \tag{13}$$

with the range of n *and the standardization as above.*

In a similar way we can adjust the statement of Theorem 3 also for some other types of systems of congruence classes mentioned in the introduction.

What concerns the range of n in the statements, the interval $n \in \{0, 1, \ldots, m-1\}$ cannot be contracted in general. This is due to the fact that there are systems of congruence classes with $m_0 = m$. On the other hand the period m_0 of the covering function $\mathfrak{m}$ is always a divisor of m, but knowing the value m_0 we know an additional piece of information on (1). For instance, if we know that $m_0 = 1$, then the system is necessarily an exact M covering system and the value M can be determined using only (12) without to checking (13). Actually, we can discover m_0 due to verification of (13) over the whole range $n \in \{0, 1, \ldots, m-1\}$. For instance, the system

$$1 \pmod 3,\ 1 \pmod 6,\ 4 \pmod 6,\ 2 \pmod 9,\ 5 \pmod 9,\ 8 \pmod 9$$

satisfies (12) (it uses the same moduli as the above exact covering ones) and fulfills (13) for $n = 0$, but is not an exact covering one.

REFERENCES

[1] BEEBEE, J.: *Bernoulli covers and exact covering systems*, Amer. Math. Monthly **99** (1992), 946–948.

[2] ERDŐS, P.—GRAHAM, R. L.: *Old and New Problems in Combinatorial Number Theory.* Monographie No. 28 de L'Enseigment Mathématique, Université Genèneve, 1980.

[3] FRAENKEL, A. S.: *A characterization of exactly covering congruences*, Discrete Math. **4** (1973), 359–366.

[4] PORUBSKÝ, Š.: *Covering systems and generating functions*, Acta Arith. **26** (1975), 223–231.

[5] PORUBSKÝ, Š.: *On m-times covering systems*, Acta Arith. **29** (1976), 159–169.

[6] PORUBSKÝ, Š.: *Identities involving covering systems I*, Math. Slovaca **44** (1994), 153–162.

[7] PORUBSKÝ, Š.—SCHÖNHEIM, J.: *Covering systems of Paul Erdős: past, present and future.* In: Proceeding of the International Conference Paul Erdős and his Mathematics Budapest 1999 (G. Halász, L. Lovász, M. Simonovits, V .T. Sós, eds.), Bolyai Soc. Math. Stud. 11, Springer Verlag / János Bolyai Math. Society, Berlin-Heidelberg-New York / Budapest, 2002, pp. 581–627.

[8] PORUBSKÝ, Š.—SCHÖNHEIM, J.: *New necessary and sufficient conditions on (a_i, m_i) in order that $x \equiv a_i \pmod{m_i}$ be a covering system*, Discrete Math. (To appear).

[9] SCHÖNHEIM, J.: *Covering congruences related to modular arithmetic and error correcting codes*, Ars Combin. **16-B** (1983), 21–25.

[10] SUN, Z.-W.: *Several results and systems of residue classes*, Math. China **18** (1989), 251–252.

[11] ZNÁM, Š.: *A simple characterization of disjoint covering systems*, Discrete Math. **12** (1975), 89–91.

Received October 10, 2002

* *Institute of Computer Science*
Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2
CZ–182 07 Prague 8
CZECH REPUBLIC
E-mail: porubsky@cs.cas.cz

** *School of Mathematical Sciences*
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL
E-mail: shanan@math.tau.ac.il