Remarks on systems of congruence classes

by

YONG-GAO CHEN (Nanjing) and ŠTĚFAN PORUBSKÝ (Prague)

Let

\[(1) \quad a_j \pmod{n_j}, \quad 0 \leq a_j < n_j, \quad j \in I, \quad 1 < \text{card}(I) < \aleph_0, \quad 0 \not\in I,\]

be a finite system of congruence classes. We refer to \(n\) as the modulus of the congruence class \(a \pmod{n}\) and to two congruence classes as congruent if there exists a translation carrying one into the other. The system (1) is called incongruent if no two of its classes are congruent. The modulus \(n_j\) is said to be a divmax (in (1)) if

\[n_j | n_i \Rightarrow n_j = n_i, \quad i \in I.\]

In particular, the largest modulus is a divmax in (1).

Let \(\mu\) be a complex valued function defined on \(I\). Then the function

\[m(n) = \sum_{j \in I} \mu_j \chi_{a_j(n_j)}(n), \quad n \in \mathbb{Z},\]

where \(\mu_j = \mu(j)\) are complex numbers, \(\chi_{a_j(n_j)}\) is the indicator of the class \(a_j \pmod{n_j}\) and \(\mathbb{Z}\) the set of all integers, is called the covering function of system (1). The system (1) is then called a \((\mu, m)\)-covering [6]. The covering function \(m\) is periodic and in what follows its least nonnegative period will be denoted by \(n_0 = n_0(\mu, m)\). Plainly, \(n_0\) is always a divisor of \(N = \text{l.c.m.}[n_j]_{j \in I}\).

If \(m(n) = 1\) for every \(n \in \mathbb{Z}\) then the \((\mu, 1)\)-coverings are just the \(\varepsilon\)-covering systems from [13]. The most studied \((\mu, m)\)-coverings are ones with constant weight function \(\mu\), namely \(\mu_j = 1\) for all \(j \in I\). If the covering function of a system (1) is also constant, say \(m(n) = m\) for every \(n \in \mathbb{Z}\), then the system (1) is called \(m\) times covering [8]. The \(m\) times covering
systems with \( m = 1 \) are traditionally called *disjoint coverings* (or *exact coverings*). If the function \( \mu \) is constant and equal to 1 and if \( m(n) \geq 1 \) for every \( n \in \mathbb{Z} \) then we obtain the so-called *covering systems*. Both last notions were introduced by P. Erdős (although he originally understood under covering systems only incongruent systems, i.e. ones with all the moduli \( n_i \) distinct, a point of view we shall not adopt here, for the sake of simplicity). Finally, if the function \( \mu \) is constant and equal to 1 but \( m(n) \leq 1 \) for every \( n \in \mathbb{Z} \) then the system (1) is called *disjoint*.

One of the first results on covering systems was the result independently proved by Mirsky, D. Newman, Davenport and Radó saying that every disjoint covering contains at least 2 congruent classes (in other words, there is no incongruent disjoint covering system). Actually, their proof implies that these are the classes with respect to the largest modulus. Znám [11] conjectured that 2 can be replaced by the least prime divisor \( p(n_s) \) of the largest modulus \( n_s \) and M. Newman [4] proved this. In [6] this result was extended to general \( (\mu, m) \)-coverings and all the divmax’s \( n_s \) which do not divide the period \( n_0 \) of the covering function \( m \) (note that \( n_j \nmid n_0 \) iff there exists an integer \( d \) with \( d \mid n_j \) and \( d \nmid n_0 \)). For disjoint coverings the lower bound was improved in [1] to

\[
\min_{j \in I, n_j \neq n_s} G\left( \frac{n_s}{(n_j, n_s)} \right),
\]

where \( G(n) \) stands for the greatest divisor of \( n \) which is a power of a single prime. Further improvement for general systems was proved by Sun [10] who removed the function \( G \) from the statement and his lower bound is

\[
\min_{j \in I \cup \{0\}, n_j \neq n_s} \frac{n_s}{(n_j, n_s)}.
\]

In the present paper we prove a result which implies all the mentioned ones.

As the first simplification in the further formulations note that we can restrict our consideration to systems (1) with identically vanishing covering function. This can be achieved after adding congruence classes \( t \ (\text{mod} \ n_0) \), \( 0 \leq t \leq n_0 - 1 \) with weights \(-m(t) = \sum_{j \in I} \mu_j \chi_{a_j(n_j)}(t)\) to the original \( (\mu, m) \)-covering (1). Then the covering function of the new system

\[
\{a_j \ (\text{mod} \ n_j) : j \in I \} \cup \{t \ (\text{mod} \ n_0) : 0 \leq t \leq n_0 - 1 \}
\]

with weights

\[
\{\mu_j : j \in I \} \cup \{-m(t) : 0 \leq t \leq n_0 - 1 \}
\]

vanishes for every \( n \in \mathbb{Z} \). This assumption technically simplifies slightly some proofs in the sense that it equalizes the position of the period \( n_0 \) with other moduli of (1).
Lemma 1 (Newton identities). Let
\[ f(x) = \prod_{j \in J} (x - x_j) = x^n + \sigma_{f,1}x^{n-1} + \sigma_{f,2}x^{n-2} + \ldots + \sigma_{f,n}, \quad n = \text{card}(J), \]
be a polynomial and
\[ h_{f,s} = \sum_{j \in J} x_j^s, \quad \tau_{f,s} = \sum_{j \in J} b_j x_j^s, \quad s = 1, 2, \ldots, \]
with \( b_j \) arbitrary complex numbers. Then
\[ h_{f,s} + \sigma_{f,1} h_{f,s-1} + \ldots + \sigma_{f,s-1} h_{f,1} + \sigma_{f,s}s = 0, \quad 1 \leq s \leq n, \]
and
\[ \tau_{f,s} + \sigma_{f,1} \tau_{f,s-1} + \ldots + \sigma_{f,n} \tau_{f,s-n} = 0, \quad s \geq n. \]

Proof. The first part is known from the so-called Newton identities and
the second follows immediately from the relation
\[ \tau_{f,s} + \sigma_{f,1} \tau_{f,s-1} + \ldots + \sigma_{f,n} \tau_{f,s-n} = \sum_{j \in J} b_j x_j^{s-n} f(x_j) = 0. \]

Theorem 1. Let (1) be a \((\mu,0)\)-covering and \( d \) a positive integer. If
there exists a complex number \( N(d) \) with the property that all the numbers
\[ \gamma_a = N(d) \sum_{d \mid n_j, j \in I \atop a_j \equiv \mu_j \text{ (mod } d)} \frac{\mu_j}{n_j}, \quad a \in \{0, 1, \ldots, d-1\}, \]
are nonnegative integers not all zero, then there exist nonnegative integers
\( c_j, \ j \in I, \) not all zero, such that
\[ \sum_{j \in I, d \mid n_j} \frac{N(d)\mu_j}{n_j} = \sum_{j \in I, d \nmid n_j} c_j \frac{d}{(d,n_j)}. \]

Proof. A simple counting and rearrangement argument (see e.g. [6] if
necessary) gives
\[ \sum_{j \in I} \frac{\mu_j z^{a_j}}{1 - z^{n_j}} = 0. \]
Let \( \omega_d = \exp(2\pi i/d) \) be a \( d \)th root of unity. Then counting the residues at
\( \omega_d^s \) in (2) we obtain
\[ \sum_{j \in I, d \mid n_j} \frac{\mu_j}{n_j} \omega_d^{sa_j} = 0, \quad s \in \mathbb{Z}. \]
Suppose that the set \( I_d \) is determined by
\[ d \mid n_j \text{ for } j \in I_d, \quad d \nmid n_j \text{ for } j \in I \setminus I_d. \]
Now, let an integer \( k \) be such that
\[
\frac{d}{(d, n_j)} \mid k, \quad j \in I \setminus I_d.
\]
We can suppose that \( k \geq 1 \). Since
\[
d \mid kn_j \iff \frac{d}{(d, n_j)} \mid k_n_j \iff \frac{d}{(d, n_j)} \mid k,
\]
we have
\[
d \mid kn_j \iff j \in I_d.
\]
Therefore the relation (3) becomes
\[
\sum_{j \in I_d} \mu_j N_j \omega^{ka_j} = 0,
\]
and consequently
\[
(5) \quad \sum_{j \in I_d} \frac{N(d)\mu_j}{n_j} \omega^{ka_j} = 0.
\]
If
\[
f(x) = \prod_{a=0}^{d-1} (x - \omega_d^a)^{\gamma_a},
\]
then
\[
h_{f,s} = \sum_{a=0}^{d-1} \gamma_a \omega_d^{sa} = \sum_{j \in I_d} \frac{N(d)\mu_j}{n_j} \omega_d^{sa_j}.
\]
Note that
\[
h_{f,0} = \sum_{a=0}^{d-1} \gamma_a
\]
is the degree of \( f \) and that
\[
h_{f, \deg(f)} = \sigma_{f, \deg(f)} = f(0) \neq 0.
\]
Therefore, if we define
\[
A(d) = \left\{ \sum_{j \in I_d, d \mid n_j} c_j \frac{d}{(d, n_j)} : c_j \text{ nonnegative integers} \right\},
\]
the proof will be finished if we show that
\[
(6) \quad s \not\in A_d \Rightarrow \sigma_{f,s} = 0.
\]
This can be proved by induction. Since \( 1 \not\in A(d) \) and \( \sigma_{f,1} = -h_{f,1} \equiv 0 \), suppose that \( s \not\in A(d) \) with \( 1 < s \leq h_{f,0} \) and that \( \sigma_{f,r} = 0 \) for each integer \( 1 \leq r < s \) with \( r \not\in A(d) \). We have to prove that \( \sigma_{f,s} = 0 \).
To do this, consider the equality (Lemma 1)
\[ h_{f,s} + \sigma_{f,1} h_{f,s-1} + \ldots + \sigma_{f,s-1} h_{f,1} + \sigma_{f,s} s = 0. \]
Now, if a positive integer \( t \) does not belong to \( A(d) \) then \( d \equiv t \pmod{n_j} \) for each \( j \in I \setminus I_d \). Then (5) implies that \( h_{f,t} = 0 \) for \( t \notin A(d) \), in particular, \( h_{f,s} = 0 \). On the other hand, the previous facts also show that \( \sigma_{f,i} h_{f,j} \neq 0 \) implies that
1. \( j \) belongs to \( A(d) \), and
2. either \( i \geq s \) or \( i \in A(d) \).
Altogether, \( \sigma_{f,i} h_{f,j} \neq 0 \) implies that either \( i \geq s \) or \( i + j \in A(d) \). Therefore (7) implies that \( \sigma_{f,s} = 0 \), and the proof is finished.

Note that in our assumptions the requirement that \( \gamma_{a} \)'s are nonnegative integers played an important role. However, we have a certain room for manipulation using the weights but then we usually have to exclude the classes with respect to the modulus \( n_0 \) which compensate our manipulations in the sense that the resulting covering function identically vanishes. One possible way to exclude the classes modulo \( n_0 \) is the following. We say that a modulus \( n_k \) of (1) is a \((\mu, m)\)-divmax if \( n_k \) is a divmax and \( n_k \nmid n_0 \), where \( n_0 = n_0(\mu, m) \).

**Corollary 1.** Let (1) be a \((\mu, m)\)-covering. Let \( L(n_j) \) denote the number of congruence classes modulo \( n_j \) in (1). If \( n_s \) is a \((\mu, m)\)-divmax and if the weights of all classes modulo \( n_s \) are equal and nonzero, then there exist nonnegative integers \( c_j, j \in I \), not all zero, such that
\[ L(n_s) = \sum_{j \in I \cup \{0\}, n_j \neq n_s} c_j \frac{n_s}{(n_j, n_s)}. \]

The proof follows from Theorem 1 by taking \( d = n_s \) and \( N(d) = n_s/\mu_s \).

Since
\[ \sum_{j \in I \cup \{0\}, n_j \neq n_s} c_j \frac{n_s}{(n_j, n_s)} \geq \min_{j \in I \cup \{0\}, n_j \neq n_s} \frac{n_s}{(n_j, n_s)} \geq \min_{j \in I \cup \{0\}, n_j \neq n_s} \frac{n_s}{(n_j, n_s)} G\left(\frac{n_s}{(n_j, n_s)}\right), \]
the lower bound of [1] \((n_0 = 1 \text{ in this case})\) and of [10] follow.

Motivated by results mentioned in the introduction a number of papers ([2], [5], [9], [12]) were devoted to the study of disjoint coverings (1) satisfying the condition (after reindexing if necessary)
\[ n_1 < n_2 < \ldots < n_{k-m+1} = n_{k-m+2} = \ldots = n_k. \]
(Some of these results are also proved for \( m \) times covering systems \([8]\).) It can be easily proved that the only divmax of a disjoint covering satisfying \((8)\) are the largest moduli. As it is proved in \([2]\) there exists a disjoint covering with 6 largest moduli and moduli
\[
n_1 = 3, \ n_2 = 6, \ n_3 = n_4 = \ldots = n_8 = 12.
\]
In this case
\[
L(12) = 6 = \frac{12}{(12, 6)} + \frac{12}{(12, 3)} = 3\frac{12}{(12, 6)},
\]
which shows that the estimation of Corollary 1 supersedes the previously known ones. Other examples of this type can be constructed. So for instance, take a \((\mu, m)\)-covering \((1)\) and two arbitrary positive integers \(b \geq 2, \ c \geq 2\). Without loss of generality we can suppose that \(n_k\) is a \((\mu, m)\)-divmax.

Then the system
\[
a_1 \ (\bmod \ n_1), \ldots, a_{k-1} \ (\bmod \ n_{k-1}), \ a_k + hn_k \ (\bmod \ bn_k), \ 0 \leq h \leq b - 1,
\]
has the same covering function \(m\) as the original one if to each of the congruence classes \(a_k + hn_k \ (\bmod \ bn_k), \ 0 \leq h \leq b - 1\), we assign the weight \(\mu'_k = \mu_k\). The modulus \(bn_k\) is again a \((\mu', m)\)-divmax. Now apply the above construction to the classes
\[
a_k + hn_k \ (\bmod \ bn_k), \ 1 \leq h \leq b - 1,
\]
using the number \(c\), thereby obtaining a new system \(a'_j \ (\bmod \ n'_j)\) with \(k' = k + (b - 1)c\) congruence classes. The modulus \(n'_{k'} = bcn_k\) is a divmax in this new system, which has the same covering function as the original one and consequently the same period \(n_0\). Since the modulus \(n'_{k'} = bcn_k\) appears as the modulus of \((b - 1)c\) congruence classes in this new system,
\[
L(n'_{k'}) = (b - 1)c = (b - 1)\frac{n'_{k'}}{(n'_{k'}, n'_k)} = (b - 1)\min_{n'_j \neq n'_{k'}} \frac{n'_{k'}}{(n'_{k'}, n'_k)}.
\]

The above construction plays a significant role in the definition of the so-called natural disjoint coverings \([7]\) and in disjoint coverings with precisely one multiple modulus. Therefore the result of the next Theorem 2 can be of some interest. But before stating this theorem we show some other consequences of Corollary 1.

In every disjoint covering we obviously have
\[
(9) \quad \sum_{i \in I} \frac{1}{n_i} = 1
\]
and the above mentioned result of Mirsky, Newman, Davenport and Radó shows that in every disjoint incongruent system \((1)\),
\[
\sum_{i \in I} \frac{1}{n_i} < 1.
\]
Erdős [3] strengthened this estimation by showing that in every disjoint incongruent system (1) we have

\[
\sum_{i \in I} \frac{1}{n_i} \leq 1 - \frac{1}{2|I|}.
\]

This result is the best possible as the system \(2^{i-1} \pmod{2^i}, 1 \leq i \leq k\), shows.

**Corollary 2.** Let (1) be a disjoint system. Then there exist positive integers \(A_i, i \in I\), such that

\[
\sum_{i \in I} \frac{A_i}{n_i} = 1.
\]

**Proof.** If (1) is a disjoint covering then (9) shows that (11) holds. So we can suppose that (1) is not a covering.

Let \(N = \text{l.c.m.}\{n_j: j \in I\}\). Add to (1), say, \(m \geq 1\) classes modulo \(2N\) in such a way that the new system is a disjoint covering. Then (9) implies

\[
\sum_{i \in I} \frac{1}{n_i} + \frac{m}{2N} = 1.
\]

Since \(2N\) is a divmax in this new disjoint covering, there exist (Corollary 1) nonnegative integers \(c_i, i \in I\), with

\[
\sum_{i \in I} c_i \frac{2N}{(n_i, 2N)} = m = 2N - 2N \sum_{i \in I} \frac{1}{n_i}.
\]

But \((n_i, 2N) = n_i\) for every \(i \in I\), which in turn implies

\[
\sum_{i \in I} c_i + \frac{1}{n_i} = 1.
\]

The last corollary implies a slight generalization of (10). Namely, if (1) is a disjoint incongruent system then there exists \(j \in I\) with

\[
\sum_{i \in I} \frac{1}{n_i} \leq 1 - \frac{1}{n_j}.
\]

Note that (10) follows from (13) by induction on \(k = |I|\). Namely, if \(n_j < 2^k\) then (10) follows immediately, in the opposite case apply the induction hypothesis to the system consisting of the classes with indices \(i \in I \setminus \{j\}\).

To prove (13) note that if (1) is a disjoint incongruent system then the result of Mirsky, Newman, Davenport and Radó implies that (1) is not a covering. In the course of the proof of (11) we saw that in this case \(A_i \geq 2\) at least for one \(i \in I\). And for such \(i\) the relation (13) follows immediately.

Also note that Corollary 2 can be applied to any subsystem of a disjoint system. For example, for every disjoint covering satisfying (8) there exist
positive integers $B_i$, $i = 1, \ldots, k - m$, with
\[
\sum_{i=1}^{k-m} \frac{B_i}{n_i} = 1,
\]
and positive integers $D_i$, $i = 1, \ldots, k - m + 1$, with
\[
\sum_{i=1}^{k-m+1} \frac{D_i}{n_i} = 1,
\]
extc.
Now we turn to the promised Theorem 2.

**Theorem 2.** Let (1) be a $(\mu,0)$-covering and $d$ a positive integer. If there exists a complex number $N(d)$ with the property that all the numbers
\[
\gamma_a = N(d) \sum_{d|n_j, j \in I} \frac{\mu_j}{n_j}, \quad a \in \{0,1,\ldots,d-1\},
\]
are nonnegative integers not all zero, then
\[
\sum_{j \in I, d|n_j} \frac{N(d)\mu_j}{n_j} = \min_{j \in I, d|n_j} \frac{d}{(d,n_j)}
\]
if and only if
\[
a \equiv b \left( \text{mod } \frac{d}{M_d} \right) \quad \text{and} \quad \gamma_a = \gamma_b = 1
\]
for all indices $a,b$ with $\gamma_a \neq 0$ and $\gamma_b \neq 0$, where
\[
M_d = \min_{j \in I, d|n_j} \frac{d}{(d,n_j)}.
\]

**Proof.** Let
\[
f(x) = \prod_{a=0}^{d-1} (x - \omega_d^a)\gamma_a.
\]
Then
\[
\deg(f) = \sum_{a=1}^{d-1} \gamma_a = \sum_{j \in I, d|n_j} \frac{N(d)\mu_j}{n_j}.
\]
If $b$ is an integer with
\[
1 \leq b < M_d = \min_{j \in I, d|n_j} \frac{d}{(n_j,d)}
\]
then (6) implies that $\sigma_{f,b} = 0$. Thus if $\deg(f) = M_d$ then the polynomial $f$ reduces to the form
\[
f(x) = x^{M_d} + \sigma_{f,M_d}.
\]
Since the numbers $\omega^a_d$ for $\gamma_a \neq 0$ are roots of $f$ and none of the numbers $\omega^a_d$ is a root of the polynomial $f'(x) = M_d x^M_d$ we obtain

$$\omega^M_d a = \omega^M_d b, \quad \gamma_a = \gamma_b = 1$$

for all $a, b$ with $\gamma_a \neq 0$ and $\gamma_b \neq 0$. Thus

$$M_d a \equiv M_d b \pmod{d} \quad \text{or} \quad a \equiv b \pmod{d/M_d} \quad \text{and} \quad \gamma_a = \gamma_b = 1$$

for all $a, b$ with $\gamma_a \neq 0$ and $\gamma_b \neq 0$.

Conversely, suppose that

$$a \equiv b \pmod{d/M_d} \quad \text{and} \quad \gamma_a = \gamma_b = 1$$

for all $a, b$ with $\gamma_a \neq 0$ and $\gamma_b \neq 0$. The number of such $\gamma$’s is at most $M_d$ because for any $a \in \{0, 1, \ldots, d-1\}$ there exist exactly $M_d$ numbers $b \in \{0, 1, \ldots, d-1\}$ with

$$a \equiv b \pmod{d/M_d}.$$
References


Received on 26.10.1993
and in revised form on 5.8.1994