1 Definition

Definition 1. A system of congruences

$$a_i + \sum_{j=1}^{k} a_j x_j \equiv 0 \pmod{m_i} \quad (1 \leq i \leq n) \quad (1)$$

is called covering system if every $x = [x_1, \ldots, x_k] \in \mathbb{Z}^k$ satisfies one of the congruences of the system. Such a system is called regular if it has no proper subsystem which is a covering system.

Definition 2. The set of integers $M = \{m_1, \ldots, m_n\}$ is good if there exist $a_i's \in \mathbb{Z}$ such that $\{a_j + \sum_{j=1}^{k} a_j x_j \equiv 0 \pmod{m_i}\}$ is covering system. We say that $m_i$ is helpful in $M$ if $M \setminus \{m_i\}$ is bad but $M$ is good.

2 General covering system

Here are principal result concerning covering systems for $\mathbb{Z}^k$.

Theorem 3. (Novak, Znam, Crittenden)

1. $M$ is good $\Rightarrow \sum_{i=1}^{n} 1/m_i \geq 1$.
2. the $r$-th congruence is essential and $m_r = \prod_{i=1}^{s} p_i^\gamma \Rightarrow n \geq 1 + \sum_{r=1}^{s} a_r(p_r - 1)$.
3. If a system of the form (1) covers a $k$-dim cube $C_k \subset \mathbb{Z}^k$ with the side length $2^n$, then it’s a covering one.

For the homogeneous covering system (i.e. $a_{ii} = 0$ for all $i$), we shall obtain the stronger form and analogue of Thm3.

Theorem 4. (Analogues for homogeneous covering systems)

For a given prime $q$ dividing $\prod_{i=1}^{s} m_i$ and a given $\gamma > 0$, let $n_\gamma = \# \{i: q^\gamma \mid m_i\}$, $\alpha = \min_{n_\gamma > 0} \gamma$, $\beta = \max_{n_\gamma > 0} \gamma$.

1. $\sum_{q^\gamma} n_\gamma / q^\gamma \geq 1$.
2. the $r$-th congruence is essential $\Rightarrow n \geq 1 + \sum_{r=1}^{s} \alpha_r(p_r - 1) + 1$.
3. $(n \geq 2)$ If a homogeneous system covers $C_k \subset \mathbb{Z}^k$ with the side length $2^n - 1$ and $0 = [0, \ldots, 0] \in C_k$, then it’s a covering one.

$(n \geq 5)$ If a homogeneous system covers $C_k \subset \mathbb{Z}^k$ with the side length $2^n - 1$, then it’s a covering one.

Remark 5. The following example shows that $2^n - 1$ cannot be replaced by $2^{n-1} - 1$ in Thm4:

$$y \equiv 0 \pmod{2}, \quad x + 2^y \equiv 0 \pmod{2^{n+1}}, \quad 0 \leq y \leq 2^n - 2$$

Moreover, for $n \leq 4$ the assertion of Thm4 does not hold. The following systems cover the segment $< 2, x, < 2, 4, x, < 2, 6, x, < 2, 10 >$ of the length 1, 3, 5, respectively.

$$x = 0 \pmod{2}; \quad x \equiv 0 \pmod{2^2}, 0 \pmod{3}; \quad x \equiv 0 \pmod{2^3}, 0 \pmod{3}; \quad x \equiv 0 \pmod{2^3}, 0 \pmod{3}; \quad x \equiv 0 \pmod{2}, 0 \pmod{3}, 0 \pmod{5}; \quad x \equiv 0 \pmod{2}, 0 \pmod{3}, 0 \pmod{5}, 0 \pmod{7}$$

(Actually, using the estimate for the Jacobsthal function, we could replace $2^n - 1$ by 2, 4, 6 or 10 for $n = 1, 2, 3, 4$, respectively.)

3 An algorithm for testing a set of integers for goodness

We consider the following decision problem for $k = 1$. For answering this problem, we construct an algorithm for testing for goodness.

Covering system

Instance: A multiset of integers $\{m_1, \ldots, m_n\}$.

Question: Do there exist integers $a_1, \ldots, a_n$ such that

$$\{x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_n \pmod{m_n}\}$$

is a covering system?

Algorithm Moduli

input $M := \{m(1), \ldots, m(n)\}$.

If $1/m(1) + 1/m(n) < 1$ then output "No", stop;
compute $L := \text{lcm}(m(1), \ldots, m(n))$;
compute prime factorization of $L := p(1)^{a(1)} \ldots p(s)^{a(s)}$;
if $s == 1$ then output "Don’t know", stop;
for $i = 1$ to $s$
sum $:= 0$;
for $j = a(i)$ to 1 step -1
compute sum $:= \text{sum} + p(i)^{a(i) - j}/(m \in M : p(i)^j | m)$;
if sum $< p(i)^{(a - j + 1)}$ then call Moduli($M \setminus \{m \in M : p(i)^j | m\}$), stop;
end;
end;
end;
for $i = 1$ to $s$
compute $M0 := \{m \in M : p(i) \notin m\}$
compute $M1 := \{m \in M : p(i) | m\}$
compute $\text{Good}_\text{Partition}_\text{Found} := \text{false}$;
for each $p(i)$-partition $M1: D(1) \cup \ldots \cup D(p(i))$ of $M1$
if Moduli($M0 \cup \{d/p(i) : d \in D(k)\}$) $== \text{"Don’t know"}$ for all $k \in \{1, \ldots, p(i)\}$
then $\text{Good}_\text{Partition}_\text{Found} := \text{true}$;
end;
if $\text{Good}_\text{Partition}_\text{Found} == \text{false}$ then output "No", stop;
end;
output "Don’t know";
end;
end;
The correctness of the algorithm follows from Thm3 and the following theorem.

Theorem 6. Write $M = M_0 \cup M_1$ where the members of $M_1$ are divisible by $p$ and those of $M_0$ are not. If $M$ is good, then there exists a partition of $M_1 = D_1 \cup \ldots \cup D_p$ such that $M_0 \cup \{d/p : d \in D_i\}$ is good for each choice of $i \in \{1, \ldots, p\}$.

Unfortunately this algorithm cannot give a positive answer: its output is either "No" or "Don’t know". But considering the sets which returned "Don’t know" as output, we could show that no regular and composite covering systems exist with fewer than 20 moduli.

References