ACTA ARITHMETICA
LIX.1 (1991)

Necessary conditions for distinct covering systems with square-free moduli

by

R. J. SIMPSON (Perth) and DORON ZEILBERGER (Philadelphia, Penn.)

A *distinct covering system* (henceforth DCS) is a set of congruences

$$a_1 \pmod{d_1},\quad a_2 \pmod{d_2},\quad \ldots,\quad a_k \pmod{d_k};\qquad d_1 < d_2 < \ldots < d_k$$

that cover the integers. For example

$$0 \pmod 2,\quad 0 \pmod 3,\quad 1 \pmod 4,\quad 5 \pmod 6,\quad 7 \pmod{12}$$

is such a system. Guy (Section F13 of [5]) gives many fascinating problems on DCS's. For instance, does a DCS exist with all moduli odd? In this paper we shall be mainly concerned with DCS's whose moduli are square free. Such DCS's exist (see [5], p. 140) but none are known to exist with moduli odd and square free. This is in spite of Erdős's conjecture [4] that for every t there is a distinct covering system in which all moduli are square-free integers all of whose prime factors are greater than p_t, the tth prime. We shall prove that if a DCS exists with all moduli odd and square-free, then the least common multiple of the moduli must be the product of at least 18 primes. This improves a result of Berger, Felzenbaum and Fraenkel [2] who showed that at least 13 primes were necessary.

The paper contains three theorems. With the first of these we show that if a DCS exists whose moduli are divisible by the primes $p_1, p_2, \ldots, p_k$, then a DCS exists in which $p_1, p_2, \ldots, p_k$ are the first k primes. If $p_1, p_2, \ldots, p_k$ are required to satisfy some constraint, such as all being odd, then we may assume that these are the k smallest primes satisfying this constraint.

In the second theorem of the paper we give a sieve theoretic lower bound on the number of integers which are left uncovered by a set of congruences with given square-free moduli.

In the third theorem we use notions connected with set partitions and Bell numbers to simplify the bound given in Theorem 2. This gives a result which can be easily applied to questions about DCS's with square-free moduli.

THEOREM 1. *Let q be a prime and suppose that $\{a_i \pmod{q^{\alpha_i} d_i}: i = 1, \ldots, k\}$, where $(q, d_i) = 1$ for each i, is a DCS, and let $q^{\alpha} P$ be the lowest common multiple of $q^{\alpha_1} d_1, \ldots, q^{\alpha_k} d_k$. Suppose that p is a prime such that $p < q$,*

$p \nmid P$. Then there exists a collection of congruences which covers the integers with moduli $p^{\alpha_1}d_1,\ p^{\alpha_2}d_2, \ldots, p^{\alpha_k}d_k$.

Proof. We construct a collection of congruences $\{a_i^* \pmod{p^{\alpha_i}d_i}:$ $i = 1, \ldots, k\}$ according to the following rules.

Suppose

(1) $$a_i \equiv e_{0,i}+e_{1,i}q+e_{2,i}q^2+ \ldots +e_{(\alpha_i-1),i}q^{\alpha_i-1} \pmod{q^{\alpha_i}}$$

where $0 \leqslant e_{j,i} < q$ for $j = 0, \ldots, \alpha_i-1$. Then let a_i^* be an integer satisfying:

(2) $$a_i^* \equiv a_i \pmod{d_i},$$

(3) $$a_i^* \equiv \begin{cases} e_{0,i}+e_{1,i}p+ \ldots +e_{(\alpha_i-1),i}p^{\alpha_i-1} \pmod{p^{\alpha_i}} & \text{if } e_{j,i} < p \text{ for } j = 0, \ldots, \alpha_i-1, \\ 0 \pmod{p^{\alpha_i}} & \text{otherwise.} \end{cases}$$

We show that this new collection covers the integers. Let m be any integer, and suppose

(4) $$m \equiv f_0+f_1p+f_2p^2+ \ldots +f_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha},$$

where $0 \leqslant f_j < p$ for $j = 0, 1, \ldots, \alpha-1$. Now there exists an integer n satisfying

(5) $$n \equiv m \pmod{P},$$

(6) $$n \equiv f_0+f_1q+ \ldots +f_{\alpha-1}q^{\alpha-1} \pmod{q^\alpha}.$$

Since the original collection covers the integers, n must belong to $a_i \pmod{q^{\alpha_i}d_i}$ for some i. Without loss of generality suppose

(7) $$n \equiv a_1 \pmod{q^{\alpha_1}d_1}.$$

Then by (6),

$$a_1 \equiv f_0+f_1q+ \ldots +f_{\alpha-1}q^{\alpha-1} \pmod{q^{\alpha_1}},$$

and so, since $\alpha_1 \leqslant \alpha$,

$$a_1 \equiv f_0+f_1q+ \ldots +f_{\alpha_1-1}q^{\alpha_1-1} \pmod{q^{\alpha_1}}.$$

But $a_1 \equiv e_{0,1}+e_{1,1}q+ \ldots +e_{(\alpha_1-1),1}q^{\alpha_1-1} \pmod{q^{\alpha_1}}$ by (1), so we have $f_j = e_{j,1}$ for $j = 0, \ldots, \alpha_1-1$ and each $e_{j,1} < p$. By (3) and (4) we then have

(8) $$m \equiv a_1^* \pmod{p^{\alpha_1}}.$$

Since $d_1|P$ we also have $m \equiv n \pmod{d_1}$ by (5), $a_1 \equiv a_1^* \pmod{d_1}$ by (2) so that:

(9) $$m \equiv a_1^* \pmod{d_1}.$$

Together (8) and (9) imply $m \equiv a_1^* \pmod{p^\alpha d_1}$, that is, m belongs to a congruence class in the new collection. This applies to every m so the new collection covers the integers as required. ∎

We will need the following

COROLLARY 1. *Let $\mathscr{P}$ be some subset of the primes. If there exists a DCS whose moduli have all prime factors in the set $\{q_1, q_2, \ldots, q_k\} \subseteq \mathscr{P}$ then we can construct a new DCS whose moduli have all prime factors in the set $\{p_1, p_2, \ldots, p_k\}$, the set of the k smallest primes in $\mathscr{P}$.*

Further, if the original DCS has square-free moduli, then so will the new DCS.

Proof. If $p_1 \neq q_1$ then the theorem says we can replace q_1 with p_1 in the prime factorisation of each modulus, and still have a DCS. We can similarly replace q_2 with p_2 and so on. ∎

Notation. Let $\mathscr{D} = \{d_1, \ldots, d_t\}$ be a sequence of (not necessarily distinct) positive integers, and let P be any common multiple of $d_1, \ldots, d_t$.

Define $M(\mathscr{D})$ to be a rational number such that the product $PM(\mathscr{D})$ is the minimum number of residues modulo P that can be left uncovered by t arithmetic progressions with common differences $d_1, \ldots, d_t$. It is clear that $M(\mathscr{D})$ is independent of P.

We further define $S(\mathscr{D})$ to be the set of all those subsequences of $\mathscr{D}$, including $\emptyset$, whose members are pairwise relatively prime.

If d is any integer then $\mathscr{D}(d)$ is the subsequence of $\mathscr{D}$ consisting of those members of $\mathscr{D}$ which are relatively prime to d.

For example, if $\mathscr{D} = \{d_1, d_2, d_3, d_4\} = \{2, 3, 3, 15\}$ then

$$S(\mathscr{D}) = \{\emptyset, \{d_1\}, \{d_2\}, \{d_3\}, \{d_4\}, \{d_1, d_2\}, \{d_1, d_3\}, \{d_1, d_4\}\},$$

$$\mathscr{D}(2) = \{d_2, d_3, d_4\}.$$

In most of the results that follow the order of the elements of a sequence $\mathscr{D}$ is immaterial and $\mathscr{D}$ can be regarded as a "multi-set". We will use the notation $D \subseteq \mathscr{D}$ to mean D is a subsequence of $\mathscr{D}$ and $\emptyset$ to be the "empty sequence". We hope this abuse of notation will not cause confusion.

We next define $X(\mathscr{D})$ by

$$X(\mathscr{D}) = \sum_{D \in S(\mathscr{D})} (-1)^{|D|} / \prod_{d \in D} d.$$

We will now prove a number of technical results concerning the function $X(\mathscr{D})$. The purpose of these is to prove Theorem 2, which states that under certain conditions $X(\mathscr{D})$ is a lower bound for $M(\mathscr{D})$.

LEMMA 1. *Let $\mathscr{D}$ be a finite sequence of positive integers with the property that*

$$\mathscr{D}_k \subseteq \mathscr{D}, \ \mathscr{D}_k \neq \mathscr{D} \ \Rightarrow \ X(\mathscr{D}_k) \geq 0.$$

If $\mathscr{D}_i$, $\mathscr{D}_j$ are such that $\mathscr{D}_i \subseteq \mathscr{D}_j \subseteq \mathscr{D}$ then

$$X(\mathscr{D}_i) \geq X(\mathscr{D}_j). \tag{10}$$

Proof. It is sufficient to show that (10) holds when $\mathcal{D}_j = \mathcal{D}_i \cup \{\delta\}$ for some $\delta \in \mathcal{D} \backslash \mathcal{D}_i$. In this case

$$X(\mathcal{D}_j) = \sum_{D \in S(\mathcal{D}_i)} (-1)^{|D|} / \prod_{d \in D} d + \sum_{D \in S(\mathcal{D}_i(\delta))} (-1)^{|D|+1} / (\delta \prod_{d \in D} d)$$
$$= X(\mathcal{D}_i) - (1/\delta) \sum_{D \in S(\mathcal{D}_i(\delta))} (-1)^{|D|} / \prod_{d \in D} d = X(\mathcal{D}_i) - (1/\delta) X(\mathcal{D}_i(\delta)).$$

Note that $\mathcal{D}_i(\delta) \subseteq \mathcal{D}_i \subseteq \mathcal{D}$, $\mathcal{D}_i(\delta) \neq \mathcal{D}$, hence $X(\mathcal{D}_i(\delta)) \geqslant 0$, by assumption. Thus $X(\mathcal{D}_j) \leqslant X(\mathcal{D}_i)$, as required. ■

LEMMA 2. *Let $\mathcal{D}$ be a finite sequence of positive integers and $\mathcal{D}_1$ a subsequence of $\mathcal{D}$ with the property that*

$$\mathcal{D}_k \subseteq \mathcal{D}_1 \Rightarrow X(\mathcal{D}_k) \geqslant 0. \tag{11}$$

Then

$$X(\mathcal{D}) \geqslant X(\mathcal{D} \backslash \mathcal{D}_1) - \sum_{d \in \mathcal{D}_1} (1/d) X(\mathcal{D} \backslash \mathcal{D}_1(d)).$$

Proof. Define $Y(\mathcal{D}, \mathcal{D}_j)$ where $\mathcal{D}_j \subseteq \mathcal{D}$ by

$$Y(\mathcal{D}, \mathcal{D}_j) = \sum_{\substack{D \in S(\mathcal{D}) \\ |D \cap \mathcal{D}_j| \leqslant 1}} (-1)^{|D|} / \prod_{d \in D} d.$$

We note that

$$Y(\mathcal{D}, \emptyset) = X(\mathcal{D}). \tag{12}$$

We first show that if $\mathcal{D}_k \subseteq \mathcal{D}_j \subseteq \mathcal{D}$ then

$$Y(\mathcal{D}, \mathcal{D}_j) \leqslant Y(\mathcal{D}, \mathcal{D}_k). \tag{13}$$

To demonstrate (13) it is sufficient to show that if $\delta \in \mathcal{D}$, $\delta \notin \mathcal{D}_k$ then

$$Y(\mathcal{D}, \mathcal{D}_k \cup \{\delta\}) \leqslant Y(\mathcal{D}, \mathcal{D}_k).$$

The position of δ in the subsequence $\mathcal{D}_k \cup \{\delta\}$ is immaterial. We have

$$Y(\mathcal{D}, \mathcal{D}_k \cup \{\delta\}) = \sum_{\substack{D \in S(\mathcal{D}) \\ |D \cap (\mathcal{D}_k \cup \{\delta\})| \leqslant 1}} (-1)^{|D|} / \prod_{d \in D} d$$
$$= \sum_{\substack{D \subseteq S(\mathcal{D}) \\ |D \cap \mathcal{D}_k| \leqslant 1}} (-1)^{|D|} / \prod_{d \in D} d - \sum_{\substack{D \in S(\mathcal{D}) \\ |D \cap \mathcal{D}_k| = 1 \\ \delta \in D}} (-1)^{|D|} / \prod_{d \in D} d$$
$$= Y(\mathcal{D}, \mathcal{D}_k) + (1/\delta) \sum_{\substack{D' \in S(\mathcal{D}(\delta)) \\ |D' \cap \mathcal{D}_k| = 1}} (-1)^{|D'|} / \prod_{d \in D'} d$$
$$= Y(\mathcal{D}, \mathcal{D}_k) - (1/\delta) \sum_{d_j \in \mathcal{D}(\delta)} (1/d_j) \sum_{D'' \in S(\mathcal{D}(\delta d_j))} (-1)^{|D''|} / \prod_{d \in D''} d$$
$$= Y(\mathcal{D}, \mathcal{D}_k) - (1/\delta) \sum_{d_j \in \mathcal{D}(\delta)} (1/d_j) X(\mathcal{D}(\delta d_j)) \leqslant Y(\mathcal{D}, \mathcal{D}_k)$$

by (11). This establishes (13).

We now show that

$$Y(\mathscr{D}, \mathscr{D}_1) = X(\mathscr{D}\backslash\mathscr{D}_1) - \sum_{d_1\in\mathscr{D}_1} (1/d_1) X(\mathscr{D}\backslash\mathscr{D}_1(d_1)). \tag{14}$$

The left hand side of (14) equals

$$\sum_{\substack{D\in S(\mathscr{D})\\ |D\cap\mathscr{D}_1|=0}} (-1)^{|D|}/\prod_{d\in D} d + \sum_{\substack{D\in S(\mathscr{D})\\ |D\cap\mathscr{D}_1|=1}} (-1)^{|D|}/\prod_{d\in D} d$$

$$= X(\mathscr{D}\backslash\mathscr{D}_1) + \sum_{d_1\in\mathscr{D}_1} (1/d_1) \sum_{D'\in S(\mathscr{D}\backslash\mathscr{D}_1(d_1))} (-1)^{|D'|+1}/\prod_{d\in D'} d$$

$$= X(\mathscr{D}\backslash\mathscr{D}_1) - \sum_{d_1\in\mathscr{D}_1} (1/d_1) X(\mathscr{D}\backslash\mathscr{D}_1(d_1)).$$

Finally we set $\mathscr{D}_k = \emptyset$, $\mathscr{D}_j = \mathscr{D}_1$ in (13) and apply (12) to get $X(\mathscr{D}) \geqslant Y(\mathscr{D}, \mathscr{D}_1)$. Applying (14) now gives the statement of the lemma. ∎

LEMMA 3. *Let $\mathscr{D}_1$ and $\mathscr{D}_2$ be sequences such that $\big((\operatorname{lcm}\mathscr{D}_1), (\operatorname{lcm}\mathscr{D}_2)\big) = 1$, where* lcm *denotes the least common multiple of the members of a sequence, and the outer parentheses denote greatest common divisor. Then*

$$X(\mathscr{D}_1 \cup \mathscr{D}_2) = X(\mathscr{D}_1)X(\mathscr{D}_2),$$

where the ordering of the members of $\mathscr{D}_1 \cup \mathscr{D}_2$ is immaterial.

Proof.

$$X(\mathscr{D}_1 \cup \mathscr{D}_2) = \sum_{D\in S(\mathscr{D}_1\cup\mathscr{D}_2)} (-1)^{|D|}/\prod_{d\in D} d$$

$$= \Big(\sum_{D_1\in S(\mathscr{D}_1)} (-1)^{|D_1|}/\prod_{d\in D_1} d\Big)\Big(\sum_{D_2\in S(\mathscr{D}_2)} (-1)^{|D_2|}/\prod_{d\in D_2} d\Big)$$

$$= X(\mathscr{D}_1)X(\mathscr{D}_2). \ \blacksquare$$

Notation: Let $\mathscr{D} = \{d_1, d_2, \ldots, d_t\}$ be a finite sequence of positive integers, define $\mathscr{D}_i$, $i = 1, \ldots, t$, by

$$\mathscr{D}_1 = \{d_1\}, \qquad \mathscr{D}_i = \mathscr{D}_{i-1} \cup \{d_i\}.$$

Then if $X(\mathscr{D}_i) > 0$ for $i = 1, \ldots, t$ we say that the sequence $\mathscr{D}$ is *regular*.

LEMMA 4. *If $\mathscr{D} = \{d_1, \ldots, d_t\}$ is regular, f is any permutation of $1, \ldots, t$, then $\{d_{f(1)}, \ldots, d_{f(t)}\}$ is regular.*

Proof. The proof uses a combination of induction and contradiction. The statement of the lemma clearly holds when $t = 1$. We assume it holds for $t < t_0$, and show by contradiction that it holds when $t = t_0$.

Assume then that the sequence $\mathscr{D} = \{d_1, \ldots, d_{t_0}\}$ is regular, but that some permutation of $\mathscr{D}$ is not. Thus there exists a subsequence $\mathscr{D}'$ of $\mathscr{D}$ such that $X(\mathscr{D}') \leqslant 0$. Let f be some permutation of $1, 2, \ldots, t_0$ and suppose that $\{d_{f(1)}, \ldots, d_{f(t_0)}\}$ is regular. Clearly $\{d_{f(1)}, \ldots, d_{f(t_0-1)}\}$ is also regular. In order to avoid a counterexample to the lemma with $t = t_0 - 1$, we must have

$d_{f(t_0)} \in \mathscr{D}'$. Thus

(15) $\{d_{f(1)}, \ldots, d_{f(t_0)}\}$ is regular, $\quad X(\mathscr{D}') \leqslant 0 \Rightarrow d_{f(t_0)} \in \mathscr{D}'$.

Now suppose g is a permutation of $1, \ldots, t_0$ such that $\{d_{g(1)}, \ldots, d_{g(t_0)}\}$ is not regular; that is, there exists some initial subsequence, $\mathscr{D}''$ say, of $\{d_{g(1)}, \ldots, d_{g(t_0)}\}$ such that $X(\mathscr{D}'') \leqslant 0$. $\mathscr{D}''$ cannot equal $\{d_{g(1)}, \ldots, d_{g(t_0)}\}$ since $X(d_{g(1)}, \ldots, d_{g(t_0)}) = X(\mathscr{D}) > 0$. If h is any other permutation such that $h(t_0) = g(t_0)$, then $\{d_{h(1)}, \ldots, d_{h(t_0)}\}$ is not regular, for if it were (15) would imply $d_{h(t_0)} = d_{g(t_0)} \in \mathscr{D}''$. This is impossible since $\mathscr{D}'' \subseteq \{d_{g(1)}, \ldots, d_{g(t_0-1)}\}$. Summarising: if $d_{g(t_0)} = d_{h(t_0)}$ then $\{d_{g(1)}, \ldots, d_{g(t_0)}\}$ is regular if and only if $\{d_{h(1)}, \ldots, d_{h(t_0)}\}$ is regular.

We can therefore partition the moduli into two classes as follows.

A modulus d_i is *good* if there exists a regular ordering of $\mathscr{D}$ which finishes with d_i, otherwise it is *bad*.

Display (15) may then be stated as:

(16) If d_i is good, $X(\mathscr{D}') \leqslant 0$ then $d_i \in \mathscr{D}'$.

Now let d_g be any good modulus, d_b be any bad modulus, and let

$$\mathscr{D}_1 = \mathscr{D} \backslash \{d_g, d_b\}.$$

Note that any ordering of $\mathscr{D}$ with d_b as the last element and d_g as the second to last element cannot be regular, by the definition of bad. It must therefore contain an initial subsequence $\mathscr{D}'$, say, such that $X(\mathscr{D}') \leqslant 0$. This initial subsequence must contain d_g by (16), and so it must be $\mathscr{D}_1 \cup \{d_g\}$. That is,

(17) $$X(\mathscr{D}_1 \cup \{d_g\}) \leqslant 0.$$

Now,

$$\begin{aligned} X(\mathscr{D}_1 \cup \{d_g\}) &= \sum_{D \in \mathscr{D}_1 \cup \{d_g\}} (-1)^{|D|} / \prod_{d \in D} d \\ &= \sum_{D \in S(\mathscr{D}_1)} (-1)^{|D|} / \prod_{d \in D} d + \sum_{D \in S(\mathscr{D}_1(d_g))} (-1)^{|D|+1} / d_g \prod_{d \in D} d \\ &= X(\mathscr{D}_1) - (1/d_g) X(\mathscr{D}_1(d_g)). \end{aligned}$$

We then have by (17),

(18) $$X(\mathscr{D}_1) - (1/d_g) X(\mathscr{D}_1(d_g)) \leqslant 0.$$

Next, since $\mathscr{D} = \mathscr{D}_1 \cup \{d_g, d_b\}$, we have $X(\mathscr{D}_1 \cup \{d_g, d_b\}) > 0$. This can be expanded in the same way as $X(\mathscr{D}_1 \cup \{d_g\})$. If d_g and d_b have a common divisor we get

(19) $$X(\mathscr{D}_1) - (1/d_g) X(\mathscr{D}_1(d_g)) - (1/d_b) X(\mathscr{D}_1(d_b)) > 0.$$

(18) and (19) imply that

$$X(\mathscr{D}_1(d_b)) < 0.$$

This is impossible in view of (16) and the fact that if $(d_g, d_b) \neq 1$ then $d_g \notin \mathscr{D}(d_b)$. Therefore we conclude that $(d_g, d_b) = 1$. This applies to any choice of a good modulus and a bad modulus. Setting

$$\mathscr{D}_g = \{d \in \mathscr{D}\colon d \text{ is good}\}, \quad \mathscr{D}_b = \{d \in \mathscr{D}\colon d \text{ is bad}\},$$

we therefore have

$$(\operatorname{lcm}(\mathscr{D}_g), \operatorname{lcm}(\mathscr{D}_b)) = 1.$$

By Lemma 3 and the requirement that $X(\mathscr{D}) > 0$ we have

$$X(\mathscr{D}_g) X(\mathscr{D}_b) > 0.$$

If $X(\mathscr{D}_b) \leqslant 0$ we would have, by (16), $\mathscr{D}_g \subseteq \mathscr{D}_b$, which is impossible. Hence,

(20) $$X(\mathscr{D}_g) > 0.$$

Now if $X(\mathscr{D}') \leqslant 0$, (16) implies that $\mathscr{D}_g \subseteq \mathscr{D}'$, that is, $\mathscr{D}' = \mathscr{D}_g \cup \mathscr{D}''$ where $\mathscr{D}'' \subseteq \mathscr{D}_b$. By Lemma 3 we have

$$X(\mathscr{D}') = X(\mathscr{D}_g) X(\mathscr{D}'').$$

We have assumed that the left-hand side is non-positive, but by (20) and the contrapositive of (16) each term on the right-hand side is positive. This is impossible, hence our assumption that $\mathscr{D}$ had an initial subsequence $\mathscr{D}'$ with $X(\mathscr{D}') < 0$ was false. The case $t = t_0$ of the lemma follows and the lemma is proven by induction. ∎

THEOREM 2. *Let $p_1, \ldots, p_n, p_{n+1}$ be a sequence of distinct prime numbers, let $\{d_1, d_2, \ldots, d_t\}$ be a finite sequence of square-free integers, each of whose prime factors belong to the given sequence. For $i = 1, \ldots, n+1$ define*

(21) $$\mathscr{D}_i = \{d_j\colon p_l | d_j \Rightarrow l \leqslant i\}.$$

Then, if

(22) $$X(\mathscr{D}_i) > 0 \quad \textit{for} \quad i = 1, \ldots, n$$

then

(23) $$M(\mathscr{D}_{n+1}) \geqslant X(\mathscr{D}_{n+1}),$$

where M was defined after Corollary 1.

Proof. The proof is by induction on n. It is easily checked for $n = 1$. We will suppose that (23) holds for all sequences satisfying (22) and consisting only of integers whose prime factors belong to the sequence $\{p_1, \ldots, p_n\}$.

Let $P = p_1 p_2 \ldots p_n$ and for convenience write $\mathscr{D}$ for $\mathscr{D}_{n+1}$ and p for p_{n+1}. To prove the theorem we must show that

$$M(\mathscr{D}) \geqslant X(\mathscr{D}).$$

Suppose we have a collection $\mathscr{A}$ of congruences, $\mathscr{A} = \{a_i \pmod{d_i}: d_i \in \mathscr{D}\}$, such that the number of residue classes modulo pP not belonging to $\bigcup \mathscr{A}$ is $pPM(\mathscr{D})$.

Fix this collection and partition $\mathscr{D}$ as

$$\mathscr{D} = \mathscr{S}_0 \cup \mathscr{S}_1 \cup \ldots \cup \mathscr{S}_p$$

where $d_i \in \mathscr{S}_0$ if and only if $(p, d_i) = 1$, and $d_i \in \mathscr{S}_j$, for $j = 1, \ldots, p$ if and only if p divides d_i and $a_i \equiv j \pmod{p}$.

For each j consider those residues modulo pP which are congruent to j modulo p and which do not belong to $\bigcup \mathscr{A}$. Let the number of such residue classes be N_j. Clearly we have

$$\sum_{j=1}^{p} N_j = pPM(\mathscr{D}). \tag{24}$$

Now fix some j. In [7] it was shown that we can use those congruence classes in $\mathscr{A}$ which intersect $j \pmod{p}$ to construct a collection of congruence classes which leave N_j residues mod P uncovered, and whose sequence of moduli is $\mathscr{S}_0 \cup \mathscr{S}_j^*$ where

$$\mathscr{S}_j^* = \{d_i/p: d_i \in \mathscr{S}_j\}.$$

The construction is performed by mapping the integers congruent to $j \pmod{p}$ onto the integers in an obvious way. Having performed this construction we consider two cases.

(a) If $\mathscr{S}_0 \cup \mathscr{S}_j^*$ is regular (the order of the elements in this sequence is immaterial by Lemma 4) then (22) is satisfied and so we may apply the induction hypothesis. Thus, using Lemma 2,

$$\begin{aligned} N_j &\geqslant PM(\mathscr{S}_0 \cup \mathscr{S}_j^*) \geqslant PX(\mathscr{S}_0 \cup \mathscr{S}_j^*) \\ &\geqslant P\{X(\mathscr{S}_0) - \sum_{d_i \in \mathscr{S}_j^*} (1/d_i) X(\mathscr{S}_0(d_i))\}. \end{aligned} \tag{25}$$

(b) If $\mathscr{S}_0 \cup \mathscr{S}_j^*$ is not regular we set

$$\mathscr{S}_0 = \{d_1, \ldots, d_m\}, \qquad \mathscr{S}_j^* = \{d_{m+1}, \ldots, d_n\}.$$

Suppose that r is the least index such that $\{d_1, \ldots, d_r\}$ is *not* regular. Now $\mathscr{S}_0 \subseteq \mathscr{D}$, $\mathscr{D}$ is regular so $\mathscr{S}_0$ is regular. So is any subsequence of $\mathscr{S}_0$. Thus $n \geqslant r > m$ and if $i < r$ we must have

$$X(\{d_1, \ldots, d_i\}) > 0.$$

On the other hand, since $\{d_1, \ldots, d_r\}$ is not regular we have

$$0 \geqslant X(\{d_1, \ldots, d_r\}) = X(\{d_1, \ldots, d_{r-1}\}) - \frac{1}{d_r} X(\mathscr{D}_r) \tag{26}$$

where

$$\mathscr{D}_r = \{d_i: 1 \leqslant i \leqslant r-1, (d_i, d_r) = 1\}.$$

Now

$$\{d_1, \ldots, d_{r-1}\} = \mathscr{S}_0 \cup \{d_{m+1}, \ldots, d_{r-1}\}.$$

Since this sequence is regular we may apply Lemma 2 and obtain

$$X(\{d_1, \ldots, d_{r-1}\}) \geqslant X(\mathscr{S}_0) - \sum_{i=m+1}^{r-1} (1/d_i) X(\mathscr{S}_0(d_i)). \tag{27}$$

Now d_r does not belong to $\mathscr{D}_r$ so $\mathscr{D}_r$ is regular, and so is $\mathscr{S}_0(d_r)$. It is easily seen that $\mathscr{S}_0(d_r) \subseteq \mathscr{D}_r$, so by Lemma 1

$$X(\mathscr{S}_0(d_r)) \geqslant X(\mathscr{D}_r). \tag{28}$$

Substituting (27) and (28) in (26) gives

$$0 \geqslant X(\mathscr{S}_0) - \sum_{i=m+1}^{r} (1/d_i) X(\mathscr{S}_0(d_i)).$$

Furthermore, for $i = r+1, \ldots, n$, $\mathscr{S}_0(d_i) \subseteq \mathscr{S}_0$ and is therefore regular. So $X(\mathscr{S}_0(d_i)) > 0$ and the sum above can be extended to include $i = r+1$ to n while preserving the inequality. Since N_j is clearly non-negative we then have

$$N_j \geqslant P\{X(\mathscr{S}_0) - \sum_{i=m+1}^{n} (1/d_i) X(\mathscr{S}_0(d_i))\} = P\{X(\mathscr{S}_0) - \sum_{d_i \in \mathscr{S}_j^*} (1/d_i) X(\mathscr{S}_0(d_i))\}.$$

This is identical to (25), so (25) holds for each j, $j = 1, \ldots, p$. By (24) we then have

$$\begin{aligned} pPM(\mathscr{D}) &= \sum_{j=1}^{p} N_j \geqslant \sum_{j=1}^{p} P\{X(\mathscr{S}_0) - \sum_{d_i \in \mathscr{S}_j^*} (1/d_i) X(\mathscr{S}_0(d_i))\} \\ &= pPX(\mathscr{S}_0) - \sum_{j=1}^{p} \sum_{d_i \in \mathscr{S}_j^*} (1/d_i) X(\mathscr{S}_0(d_i)) \\ &= pP\{X(\mathscr{S}_0) - \sum_{\substack{\delta \in \mathscr{D} \\ p \mid \delta}} (1/\delta) X(\mathscr{S}_0(\delta))\} \\ &= pP\{X(\mathscr{S}_0) - \sum_{\substack{\delta \in \mathscr{D} \\ p \mid \delta}} (1/\delta) X(\mathscr{D}(\delta))\} = pPX(\mathscr{D}), \end{aligned}$$

as required. ∎

We now prove our third theorem.

THEOREM 3. *If P has prime factorisation*

$$P = \prod_{i=1}^{t} p_i^{\alpha_i}$$

and $\mathscr{D}$ is the set of all distinct divisors of P excluding 1, *and*

(i) $x_j = p_j^{-1} + \ldots + p_j^{-\alpha_j}$ *for* $j = 1, \ldots, t$,

(ii) $\sigma_0, \sigma_1, \ldots, \sigma_r$ *are the elementary symmetric functions in* $x_1, \ldots, x_r$: $(t+x_1)\ldots(t+x_r) = \sigma_0 t^r + \ldots + \sigma_r$,

(iii) A_n *is the integer sequence generated by the recurrence*

$$A_n = -\sum_{k=0}^{n-1} \binom{n-1}{k} A_k, \quad A_0 = 1 \quad (\{A_k\} = \{1, -1, 0, 1, 1, -2, -9, -9, 50, \ldots\})$$

then

$$X(\mathscr{D}) = \sum_{j=1}^{t} A_j \sigma_j.$$

Proof.

$$X(\mathscr{D}) = \sum \frac{(-1)^k}{d_1 \ldots d_k} \tag{29}$$

where the sum ranges over all sets $\{d_1, \ldots, d_k\}$ of divisors of P that are pairwise relatively prime. The right-hand side of (29) is equal to

$$\sum_{m|P} (1/m) \sum (-1)^k \tag{30}$$

where the inner sum ranges over all sets $\{d_1, \ldots, d_k\}$ of divisors of P which are pairwise relatively prime and whose product is m.

Consider now any divisor m of P and let its prime factorisation be

$$p_{i_1}^{\alpha_{i_1}} \ldots p_{i_s}^{\alpha_{i_s}}$$

and

$$L = \{p_{i_1}, \ldots, p_{i_s}\} \subseteq \{p_1, \ldots, p_r\}.$$

Now any factorisation of m corresponds to a set partition of L, so the inner sum in (30) corresponds to

$$\sum_{\text{set partitions of } L} (-1)^{\text{number of sets in partition}}. \tag{31}$$

But set partitions ring a bell: the famous Bell numbers enumerate the total number of set partitions of an n-element set. They satisfy the famous recurrence:

$$B_n = \sum_{k=0}^{n-1} \binom{n-1}{k} B_k, \quad B_0 = 1. \tag{32}$$

The usual way to prove (32) is to consider the set to which the nth element belongs. It may have any number of companions from 0 to $n-1$, say $n-1-k$ companions, and the number of ways of choosing them is

$$\binom{n-1}{n-1-k} = \binom{n-1}{k}.$$

The remaining k elements can be partitioned in B_k ways.

To get (31), however, we need "weighted counting" where each set partition gets, not weight 1, but weight $(-1)^{\text{number of sets}}$; calling these new numbers A_n, the same argument that yielded (32) gives

$$A_n = -\sum_{k=0}^{n-1} \binom{n-1}{k} A_k, \quad A_0 = 1.$$

(The minus sign in front of the sum is due to the fact that by deleting the set to which n belonged we "lost" a set and thus changed the sign of the partition.)

Thus (31) is equal to $A_{|L|}$. From (29) and (30) we then have

$$X(\mathscr{D}) = \sum_{L \subseteq \{p_1, \ldots, p_r\}} \left(\sum_{p_i | n \Rightarrow p_i \in L} \frac{1}{n} \right) A_{|L|}. \tag{33}$$

If $L = \{p_{i_1}, \ldots, p_{i_s}\}$, the inner sum is clearly equal to $x_{i_1} \ldots x_{i_s}$. Thus (33) becomes

$$\sum_{\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, r\}} x_{i_1} \ldots x_{i_s} A_s = \sum_{s=0}^{r} \sigma_s A_s.$$

This completes the proof. ∎

COROLLARY 2. *Any DCS consisting of odd square-free moduli must involve at least* 18 *different prime divisors.*

Proof. We show that no DCS can exist whose moduli have an lcm divisible by at most 17 distinct primes. By Corollary 1 it is sufficient to show that no DCS exists whose lcm divides the product of the first 17 odd primes: 3, 5, ..., 61.

Trying the products 3, 3·5, 3·5·7, ..., 3·5·...·61 as P in Theorem 3 we get $X(\mathscr{D})$ positive in each case. When P is the product of the first 17 odd primes we get $X(\mathscr{D}) = 0.002596\ldots$ Applying Theorem 2 we therefore have $M(\mathscr{D}) > 0$ when $\mathscr{D}$ is the set of divisors greater than 1 of this P. Thus no DCS can exist with this set of divisors. ∎

Remarks. Corollary 2 gives the best result to date. [1] gave 11 primes and [2] 13 primes compared with our 18.

The disappointing feature of this work is that we have not been able to extend Theorem 2 to apply to non-square-free moduli. We believe this is possible; if we are able to do so it will be the subject of a subsequent paper. With the exceptions of Theorem 2 and Corollary 2 all results herein apply to non-square-free moduli.

Acknowledgement. One of us (Zeilberger) would like to thank Marc Berger and Aviezri Fraenkel for introducing him to this fascinating subject. Thanks are also due to C. E. Krukenberg and John Selfridge for helpful discussions.

References

[1] Marc A. Berger, Alexander Felzenbaum, and Aviezri S. Fraenkel, *Necessary condition for the existence of an incongruent covering system with odd moduli*, Acta Arith. 45 (1985), 375–379 and 48 (1987), 73–79.
[2] –, –, –, *New results for covering systems of residue sets*, Bull. Amer. Math. Soc. 14 (1986), 121–125.
[3] R. F. Churchhouse, *Covering sets and systems of congruences*, in *Computers in Mathematical Research* (R. F. Churchhouse and J. C. Hertz, eds.), North-Holland, Amsterdam 1968, pp. 20–36.
[4] P. Erdős, *Problems and results in combinatorial number theory III*, in *Number Theory Day*, Lecture Notes in Math. 626, Springer, 1976, pp. 43–72.
[5] Richard K. Guy, *Unsolved Problems in Number Theory*, Springer, New York 1981.
[6] C. E. Krukenberg, Ph.D. thesis, Univ. of Illinois, 1971. (Available from University Microfilms, Ann Arbor, Michigan.)
[7] R. J. Simpson, *Regular coverings of the integers by arithmetic progressions*, Acta Arith. 45 (1985), 145–152.

SCHOOL OF MATHEMATICS AND STATISTICS
CURTIN UNIVERSITY OF TECHNOLOGY
P.O. Box U 1987
Perth WA 6001
Australia

DREXEL UNIVERSITY
Philadelphia, Pennsylvania
USA

Received on 30.10.1989 (1981)