SURVEY ON COVERING CONGRUENCES

THOMAS ZAMOJSKI

Abstract. This survey begins with the problem that motivated the concept of covering congruences. We then put emphasis on late developments, in the 80's, made principally by Berger, Felzenbaum, Fraenkel, Erdös and Graham, but we make note of historical developments leading there

1. Origin of covering systems

Definition 1. $\mathcal{S} = \{a_i \pmod{n_i}\}_{1 \leq i \leq k}$ is called a covering system of congruences (CS) if every integer satisfies at least one of the congruences and k is finite. We denote the classes of $\mathcal{S}$ as $\mathcal{A}_i$

This curious and elegant concept of a covering system came from somewhat unexpectedly a very reasonable problem given by Romanoff. The later asked in 1934 no one else than P. Erdös for a solution to his problem, that he had but partially solved. The problem was the following: Are there infinitely many odd integers not of the form $p + 2^m$ where p is prime? It is in 1950 that Erdös [5] constructed an infinite arithmetic sequence of odd integers not representable as $2^m + p$ using a CS . The construction we shall give now:

Proof. Suppose we have a covering system $\mathcal{S}$ like the following

$$\{a_i \pmod{ord_{p_i} 2)\}_{1 \leq i \leq k}$$

where p_i are distinct odd primes.
Since p_i are pairwise relatively prime, by the Chinese Remainder Theorem (CRT), the system of congruences

$$x \equiv 2^{a_i} \pmod{p_i},\ 1 \leq i \leq k$$
$$x \equiv 1 \pmod{2}$$

has a solution (mod $2.\prod_{i=1}^{k} p_i$). Therefore there is a smallest nonnegative integer n_o solution to the system. For any $n \equiv n_o (\text{mod } 2.\prod_{i=1}^{k} p_i)$ and a given integer j, we have $j \equiv a_i (\text{mod } ord_{p_i} 2)$ for at least one i since $\mathcal{S}$ is a covering system. So

Date: March, 2002.

$$n - 2^j \equiv n_o - 2^{a_i} \equiv 0 \quad (mod\ p_i) \Rightarrow$$
$$\Rightarrow \text{if } n - 2^j > p_i, \text{ it is composite}$$
$$\text{and if it is true } \forall \text{ j with } 2^j < n, \text{ then } n \neq 2^m + p.$$

We do not have to worry about the exceptional case $n - 2^j = p_i$ for some i and j since we can always impose an extra congruence condition in $\mathcal{S}$ to avoid it. Remains to construct $\mathcal{S}$, which Erdös did as follows:

$$0(\text{mod } 2),\ 0(\text{mod } 3),\ 1(\text{mod } 4),\ 3(\text{mod } 8),\ 7(\text{mod } 12),\ 23(\text{mod } 24)$$

where

$$2 = ord_3\, 2,\ 3 = ord_7\, 2,\ 4 = ord_5\, 2,\ 8 = ord_{17}\, 2,\ 12 = ord_{13}\, 2,\ 24 = ord_{241}\, 2.$$

With this, we get, after working out CRT, the arithmetic sequence 7629217 (mod 11184810), which contains no integer of the form $2^m + p$. □

This is a very impressing result, and a glorious birth for covering congruences. It shows right from the start its power in problem solving, especially where some sort of construction as above is involved. With this result in hand, Erdös began to tackle generalisation of Romanoff's problem, as well as to exploit his newly thought concept to raise problems (so typical of him) and to open new path of research. This lead people to study special type of CS, which we turn up to now.

2. DISJOINT COVERINGS

Definition 2. A CS $\mathcal{D}$ is called disjoint (DCS) if it partitions $\mathbb{Z}$, i.e. every integer belongs to *exactly* one class in $\mathcal{D}$.

We reorder the moduli of $\mathcal{D}$ if needed to get $n_1 \leq ... \leq n_k$. Amongst the different types of coverings we will see, this one is somewhat the one with the strongest condition imposed on it, and therefore it seems natural that there are in fact more results on these coverings then in any other domain. As we shall see, we can pin down precisely a large amount of such systems. But first, 2 elementary observations that will become handy later on.

$$(n_i, n_j) > 1 \qquad \textit{and} \qquad \sum_{i=1}^{k} n_i^{-1} = 1 \tag{1}$$

Proof. If $(n_i, n_j) > 1$, then by CRT, $\exists\, x \in \mathbb{Z}/n_i n_j \mathbb{Z}$ satisfying $x \equiv a_i\ (mod\, n_i)$ and $x \equiv a_j\ (mod\, n_j)$ simultaneously.
Now, the density of $\mathcal{A}_i = d(\mathcal{A}_i) = n_i^{-1}$. Since $\mathcal{S}$ covers $\mathbb{Z}$,

$$d(\mathcal{S}) = d(\bigcup_{i=1}^{k} \mathcal{A}_i) = 1.$$

Since $\mathcal{S}$ is disjoint,

$$d(\bigcup_{i=1}^{k} \mathcal{A}_i) = \sum_{i=1}^{k} d(\mathcal{A}_i) = \sum_{i=1}^{k} n_i^{-1}.$$

Hence $\sum_{i=1}^{k} n_i^{-1} = 1$ □

$$\frac{1}{1-z} = \sum_{i=1}^{k} \frac{z^{a_i}}{1-z^{n_i}}, \qquad where\ z \in \mathbb{C},\ |z| < 1 \tag{2}$$

Proof.

$$\sum_{i\in\mathbb{N}} z^i = \sum_{i=0}^{\infty} z^i = \frac{1}{1-z},\ since\ \mid z \mid < 1.$$

$$Also\ \sum_{i\in\mathbb{N}} z^i = \sum_{i=1}^{k} \sum_{j\in\mathcal{A}_i} z^j = \sum_{i=1}^{k} z^{a_i} \sum_{j\in\mathbb{N}} (z^{n_i})^j = \sum_{i=1}^{k} \frac{z^{a_i}}{1-z^{n_i}}$$

$$Hence\ \frac{1}{1-z} = \sum_{i=1}^{k} \frac{z^{a_i}}{1-z^{n_i}}$$

□

These results are due to Erdös and Graham. But the first major result on disjoint covering, found by Mirsky and Newman and independently by Davenport and Rado [6], is that in a DCS, we must have $n_{k-1} = n_k$. Their proof introduces roots of unity in the subject, which became an important part of the study of DCS. They argumented that if we let in (2) $z \to \omega$, a primitive n_k-th root of unity, say $e^{\frac{2\pi i}{n_k}}$, and that $n_{k-1} < n_k$, then the left hand side and the first $k-1$ terms on the right converges to a finite number, but the last term $\frac{z^{a_k}}{1-z^{n_k}} \to \infty$, a contradiction. This result was improved latter on by Newman [9] and independently by Znam [13], using similar arguments. They proved analytically, using (2) and roots of unity, that we must have in fact $n_{k-p(N)+1} = ... = n_{k-1} = n_k$, where $N = lcm(n_1, ..., n_k)$ and p(N) is the least prime divisor of N. But it seems artificial to introduce complex numbers and limits in an elementary problem, and so in that sense, the proof discovered in 1986 by Marc.A.Berger, Alexander Felzenbaum and Aviezri Fraenkel (BFF) is much more satisfying since it is geometrical. Furthermore, their key insight allowed them to extend a lot of old results in an elegant way; in particular, they extended the Newman-Znam result mentioned above:

Theorem 1. [1] *Let $\mathcal{D}$ be a DCS. Then any maximal modulus n is repeated at least p(N) times, where maximal is in the sense of division, i.e. if $n|n_i$, then $n = n_i$.*

Their proof resides on cell partition of a parallelotope and coset partition of σ_N. Let $N = \prod_{j=1}^{m} p_j^{r_j}$. Then remodulising (mod N) the congruences in $\mathcal{D}$ (e.g. 1 (mod 2) becomes $1 or 3$ (mod 4)), we get every integer of $[0, N-1]$ exactly once. We use two maps here to parallelotopes:
Using CTR:

$$[0, N-1] \to [0, p_1^{r_1} - 1] \times ... \times [0, p_m^{r_m} - 1]$$

Using p-ary representation, $b \in [0, p_j^{r_j} - 1]$, $b = \sum_{j=0}^{m-1} b_j p^j$:

$$[0, p_j^{r_j} - 1] \to [b_{m-1}, ..., b_0]$$

With this way of seeing the problem and with previous results on parallelotope partitions, the theorem follows beautifully.

2.1. **Parallelotope Partition.** [1]

Let $\vec{b} = (b_1, ..., b_n) \in \mathbb{Z}^n$, with $b_i \geq 2$. Then a parallelotope $\mathcal{P}$ is

$$\begin{aligned}\mathcal{P}(n; \vec{b}) &= \{\vec{c} = (c_1, ..., c_n) \in \mathbb{Z}^n : \; 0 \leq c_i \leq b_i\} \\ &= B_1 \times ... \times B_n, \; where \; B_i = \{0, ..., b_i - 1\}\end{aligned}$$

Let $\vec{u} = (u_1, ..., u_n) \in \mathcal{P}$ be arbitrary. A cell $\mathcal{K}$ of $\mathcal{P}$, with index set $I(\mathcal{K})$, $I \subseteq \{1, ..., n\}$ is

$$\begin{aligned}\mathcal{K} &= \{\vec{s} = (s_1, ..., s_n) \in \mathbb{Z}^n : 0 \leq s_i \leq b_i, \; for \; i \in I, \quad s_i = u_i, \; for \; i \notin I\} \\ &= D_1 \times ... \times D_n, \quad where \; D_i = \{0, ..., b_i - 1\} \; for \; i \in I, \; D_i = \{u_i\} \; for \; i \notin I\end{aligned}$$

Let τ be a cell-partition of $\mathcal{P}$, then $\mathcal{K} \in \tau$ is called minimal (subset minimal) if $\mathcal{K}_i \in \tau$, $I(\mathcal{K}_i) \subseteq I(\mathcal{K}) \Rightarrow I(\mathcal{K}_i) = I(\mathcal{K})$. The main fact we need is the following:

Lemma 1. *If τ is a cell-partition of $\mathcal{P}$ into at least 2 cells and $\mathcal{E} \in \tau$ is minimal, then τ contains at least b $I(\mathcal{E})$-cells, where $b = min\{b_i : i \notin I(\mathcal{E})\}$.*

Proof: Suppose $\mathcal{E}$ is a singleton, i.e. $I(\mathcal{E}) = \varnothing$. Each direction has at least length b, so there exists a cube C of volume b^n such that it contains $\mathcal{E}$. $\tau_1 = \{\mathcal{K} \cap C \mid \mathcal{K} \in \tau\}$ is a cell-partition of C induced by τ. The volume $V(\mathcal{K})$ of a cell $\mathcal{K}$ of C is $b^{\#I(\mathcal{K})}$, but because τ_1 is a cell-partition:

$$\sum_{\mathcal{K} \in \tau_1} V(\mathcal{K}) = b^n$$

$$\text{Also} \sum_{\mathcal{K} \in \tau_1} V(\mathcal{K}) \equiv \# \text{ of singletons} \pmod{b} \Rightarrow$$

$$\Rightarrow \# \text{ of singletons} \mid b$$

Since there is 1 singleton in C, there are at least b of them.

Now if $\mathcal{E}$ is not a singleton, then let π = projection of $\mathcal{P}$ through $I(\mathcal{E})$. Then $\pi(\mathcal{E})$ is a singleton and $\pi(\tau)$ is a cell-partition. Therefore, we are in the previous situation, and $\exists \mathcal{K}_1 ... \mathcal{K}_b$ such that $\pi(\mathcal{K}_i)$ is a singleton. It follows that $I(\mathcal{K}_i) \subset I(\mathcal{E}) \Rightarrow I(\mathcal{K}_i) = I(\mathcal{E})$ by minimality of $\mathcal{E}$. □

2.2. **Cosets.** [1]

It is somewhat easier to think of congruences as cosets of a cyclic group, at least it helps in proofs concerning DCS. Let σ_N be a cyclic group of order N under addition (mod N), where $N = lcm(n_1, ..., n_k) = \prod_{j=1}^{m} p_j^{r_j}$ as usual. Then $H_i = n_i . \sigma_N$ is a subgroup of σ_N and $C_i = a_i + H_i$ is a coset. Thus, $\mathcal{D} = \{a_i \; (mod \; n_i)\} = \{C_i\}$ is a coset partition of σ_N. We reintroduce our mappings mentioned above. Here, $0 \le s_j \le p_j^{r_j}$ and $0 \le b_x^{(j)} \le p_j$. By p-ary representation:

$$s \equiv s_j \ (mod\ p_j^{r_j}) = \sum_{x=1}^{r_j} b_x^{(j)} p_j^{r_j - x}$$

$$\mathbf{\Psi}^{(j)}(s) = (b_1^{(j)}, ..., b_{r_j}^{(j)})$$
$$\mathbf{\Phi}(s) = (\mathbf{\Psi}^{(1)}(s), ..., \mathbf{\Psi}^{(m)}(s))$$

So according to this definition, we have:

$$\mathbf{\Phi} : \sigma_N \to \mathcal{P}(\sum_{j=1}^{m} r_j; \underbrace{p_1, ..., p_1}_{r_1}, ..., \underbrace{p_m, ..., p_m}_{r_m}).$$

Now, we define addition on $\mathcal{P}$ coordinatewise. Note that coordinates are elements of different structures; the first r_1 are $\in \mathbb{Z}/p_1\mathbb{Z}$, and so on. Our main result here is that cosets become cells.

Lemma 2.
(i) $\mathbf{\Phi}$ *is bijective*
(ii) $\mathbf{\Phi}$ *is additive (mod N):* $\mathbf{\Phi}(s+t) = \mathbf{\Phi}(s) + \mathbf{\Phi}(t)$
(iii) C_i *a coset of* H_i, $|H_i| = p_1^{q_1}...p_m^{q_M}$ *then* $\mathbf{\Phi}(C_i)$ *is a cell in* $\mathcal{P}$ *and* $|\mathbf{\Phi}(C_i)| = |C_i| = |H_i|$

Proof. (i)

$$\mathbf{\Phi}(s) = \mathbf{\Phi}(t) \Rightarrow \mathbf{\Psi}^{(j)}(s) = \mathbf{\Psi}^{(j)}(t),\ 1 \le j \le m$$

$\Rightarrow$ each component in p-ary representation of $s_j,\ t_j$ are equal, by uniqueness of p-ary representation
$\Rightarrow s = t$ by CRT (here we pass from (mod p_j) to (mod N))

(ii) by definition of addition, $\mathbf{\Phi}$ is additive if and only if $\mathbf{\Psi}^{(j)}$ is additive. Addition for the p-ary representations is defined as usual, that is coordinatewise and if any of the coordinates $\ge p_j$, then we substract from it p_j and add one to the previous coordinate (or digit). Here, if the first digit $\ge p_j$, then there is no previous digit to add 1 to, so we just ignore it and still substract p_j to the first digit. With this addition operation, we have $\mathbf{\Psi}^{(j)}(s+t) = \mathbf{\Psi}^{(j)}(s) + \mathbf{\Psi}^{(j)}(t)$ and so $\mathbf{\Phi}$ is additive.

(iii) by (ii), $\mathbf{\Phi}(C_i) = \mathbf{\Phi}(H_i) + \mathbf{\Phi}(a_i)$. Since $p_j^{q_j} \mid \#H_i \Rightarrow p_j^{r_j - q_j} \mid n_i$, the last $r_j - q_j$ terms in p-ary expension of n_i are 0. Thus

$$\mathbf{\Psi}^{(j)}(H_i) = (b_1^{(j)}, ..., b_{q_j}^{(j)}, \underbrace{0, ..., 0}_{r_j - q_j})$$

Because $\mathbf{\Phi}$ is bijective, $\mid \mathbf{\Psi}^{(j)}(H_i) \mid = p_j^{q_j}$
Moreover, each $b^{(j)}$ has p_j possible value, hence there are $p_j^{q_j}$ possible elements in $\mathbf{\Psi}^{(j)}(H_i)$, which is exactly its size, and since every elements are

distinct, all of them are actually in $\mathbf{\Psi}^{(j)}(H_i)$. This tells us that $\mathbf{\Phi}(H_i)$ is a cell and so is $\mathbf{\Phi}(C_i)$. The last part follows easily. □

proof (BFF) of theorem 1. Recall that $\#C_i = N/n_i$. Suppose n_i is maximal. So

$$n_j.\#C_j = n_i.\#C_i \;\Rightarrow\; if\ \#C_j \mid \#C_i,\ then \#C_j = \#C_i$$

Let $\mathbf{\Phi}(C_i) = \mathcal{K}_i$, $\mathbf{\Phi}(C_j) = \mathcal{K}_j$ be cells and $I(\mathcal{K}_j) \subseteq I(\mathcal{K}_i)$. Then

$$\#\mathcal{K}_j \mid \#\mathcal{K}_i \;\Rightarrow\; \#C_j \mid \#C_i \;\Rightarrow\; \#C_j = \#C_i \;\Rightarrow I(\mathcal{K}_j) = I(\mathcal{K}_i)$$

Thus $\mathcal{K}_i$ is minimal. By Lemma 1, there are b minimal cells with same index. Recall that $b = min\{b_j : j \notin I(\mathcal{K}_i)\}$. According to our mapping, $j \in I(\mathcal{K}_i) \iff \mathbf{\Psi}^{(j)}(H_i) = (0, ..., 0)$, which happened whenever $r_j = q_j$. So

$$\begin{aligned} b &= min\{p_j : p_j^{r_j} \nmid |\mathcal{K}_i|\} \\ &= min\{p_j : p_j | n_i\} \qquad\qquad (since\ n_i.|\mathcal{K}_i| = N) \\ &= p(n_i) \end{aligned}$$

□

That is the insight that revolutionalised our way of approaching DCS. These kind of links between different areas of mathematics always bring guenine thoughts and a better understanding of why a certain behaviour is happening. New results pored down the pen of BFF, in particular yet another generalisation of the same theorem, that we shall but state here

Remark 1. The multiplicity of a modulus is the number of classes with this modulus. The multiplicity of a DCS is the maximum multiplicity fo its moduli.

Theorem 2. [2] *The multiplicity of any modulus n is at least*

$$m_1 = \min_{n_i \neq n} \Lambda\big(\frac{n}{(n, n_i)}\big)$$

The multiplicity of $\mathcal{D}$ is at least

$$m_2 = \big[\frac{P(N)\varphi(N)}{N}\big] + 1$$

$$\begin{array}{lll} & \Lambda(m) & = \textit{greatest divisor of } m \textit{ which is a power of a single prime} \\ \textit{where} & P(m) & = \textit{greatest prime divisor of } m \\ & \varphi(m) & = \textit{Euler's totient function} \end{array}$$

Remark 2. $m_1 \geq p(N)$, hence it englobes the previous theorem

2.3. **Characterisation of DCS.** An immediate question raised by such theorem is what form does a DCS with a single multiple modulus take? This question was already investigated by Stein [12], Znam [14] and Porubsky [10] but again, BFF [3] extended their work. Following BFF's method, we first reduce the possibilities from infinite to finite following the 2-add, 2-drop procedure. Given a DCS with moduli $(n_1, ..., n_k)$, we can form a new DCS with moduli $(2, 2n_1, ..., 2n_k)$ where a_i, n_i are doubled and 1 (mod 2) is annexed. This is referred to as the 2-add. The 2-drop is the inverse; if $n_1 = 2$, then by (1) all moduli must be even, and if $k \geq 3$ (i.e. the system is not $0, 1 \pmod 2$), the trivial one) then we form the system with moduli $(\frac{1}{2}n_1, ..., \frac{1}{2}n_k)$ and a's are replaced by $\frac{1}{2}a_i$, or $\frac{1}{2}(a_i + 1)$, whichever is an integer. It is not difficult to see that the 2-add or 2-drop procedure conserves the DCS property.

This means that a DCS with one multiple modulus, that is $n_1 < n_2 < ... < n_{k-m+1} = ... = n_k$ are characterised as those which are obtained by any number (including 0) of repetition of the 2-add procedure on the trivial system or on those satisfying

$$3 \leq n_1 < n_2 < ... < n_{k-m+1} = ... = n_k \tag{3}$$

Theorem 3. *DCS satisfying (3) and $m \leq 12$ are characterised as follows BFF contribution* [3]*:*

$$m = 4 \quad n_1 = 3,\ n_5 = 6;$$

$$m = 6 \begin{cases} n_1 = 4,\ n_7 = 8, \\ n_1 = 3,\ n_7 = 9, \\ n_1 = 3,\ n_2 = 6,\ n_8 = 12; \end{cases}$$

$$m = 7 \begin{cases} n_1 = 4,\ n_2 = 6,\ n_9 = 12, \\ n_1 = 3,\ n_2 = 6,\ n_3 = 9,\ n_{10} = 18; \end{cases}$$

$$m = 8 \begin{cases} n_1 = 5,\ n_9 = 10, \\ n_1 = 3,\ n_9 = 12; \end{cases}$$

$$m = 9 \begin{cases} n_1 = 4,\ n_{10} = 12, \\ n_1 = 3,\ n_2 = 6,\ n_{11} = 18, \\ n_1 = 4,\ n_2 = 6,\ n_3 = 8,\ n_4 = 12,\ n_{13} = 24 \\ n_1 = 3,\ n_2 = 6,\ n_3 = 9,\ n_4 = 12,\ n_5 = 18,\ n_{14} = 36 \end{cases}$$

Simpson and Zeleke contribution [11]*:*

$$m = 10 \begin{cases} n_1 = 6,\ n_{11} = 12, \\ n_1 = 3,\ n_{11} = 15, \\ n_1 = 4,\ n_2 = 8,\ n_{12} = 16, \\ n_1 = 3,\ n_2 = 9,\ n_{12} = 18, \\ n_1 = 3,\ n_2 = 6,\ n_3 = 12,\ n_{13} = 24; \end{cases}$$

$$m = 11 \begin{cases} n_1 = 4,\ n_2 = 6,\ n_3 = 8,\ n_{14} = 24, \\ n_1 = 3,\ n_2 = 6,\ n_3 = 9,\ n_4 = 12,\ n_{15} = 36; \end{cases}$$

$$m = 12 \begin{cases} n_1 = 7, \ n_{13} = 14, \\ n_1 = 5, \ n_{13} = 15, \\ n_1 = 4, \ n_{13} = 16, \\ n_1 = 3, \ n_{13} = 18, \\ n_1 = 3, \ n_2 = 6, \ n_{14} = 24, \\ n_1 = 4, \ n_2 = 6, \ n_3 = 12, \ n_{15} = 24, \\ n_1 = 3, \ n_2 = 6, \ n_3 = 9, \ n_4 = 18, \ n_{16} = 36. \end{cases}$$

This theorem is very lengthy to prove since it breaks up in many cases, but we give here an intuition of where it comes from. (1) and (2) are rephrase in terms of coset partition as follows:

$$[\ |C_i|, |C_j|\ ] < n, \qquad \sum_{i=1}^{k} |C_i| = n \tag{4}$$

$$\frac{N}{3} \geq | C_1 | \geq | C_2 | \geq ... \geq | C_{k-m+1} | = ... = | C_k | = 1 \tag{5}$$

Suppose we want to find the possible coset partition (satisfying (4) and (5)) for N=18. The possible values for $| C_i |$ are the divisors (except 1) of 18, which are $2, 3, 6, 9, 18$. By (5) $| C_i | \leq 6$, hence 9 and 18 are discarded. The possible sets we can make are $\{2\}, \{3\}, \{6\}, \{2,3\}, \{2,6\}, \{3,6\}, \{2,3,6\}$. But (4) imples that the sum of the coset of size > 1 is $N - m$, and since $m \leq 12$, this sum is ≥ 6. Hence, we must discard $\{2\}, \{3\}, \{2,3\}$ as well. The remaining possibilities correspond to a partition in the theorem, like $\{2,3,6\}$ corresponds to $| C_1 | = 6,\ | C_2 | = 3,\ | C_3 | = 2$ and the remaining 7 are of size 1. Similarly, for $N = 6, 8, 9, 12, 14, 15, 16, 18, 24,$ *or* 36, we construct all the above mentioned DCS, so the theorem states that these are the only possible values for N. And that is where it becomes lengthy to prove.

3. Other Results and Problems

As noted in the previous section, most of the results in this field of study are concerning DCS, so this section will be less rich in some sense, but there are still guenine things we have not touched yet, notably two problems at the heart of the matter.

3.1. **Incongruent Systems.** These are systems satisfying $n_1 < n_2 < ... < n_k$. Recall that a DCS must have at least $n_{k-1} = n_k$, therefore incongruent systems are completely different, not only in definition. The 2 main open problems concerns these systems and were both given by P. Erdös [7].

Open Problem 1. *For any c, is there an incongruent system with* $n_1 \geq c$*?*

Choi [4] holds the current record with a construction of such a system with $n_1 = 20$. Returning to Romanoff's problem, which motivated the concept of covering systems, we can ask a more general question: Is there an arithmetic sequence no term of which is of the form $2^m + p_1p_2...p_x$? By similar argument as the construction of Erdös, given at the beginning, one can show that if open problem 1 is true, then the answer is affirmative. This demonstrate the importance of such a question. The second problem is equally interesting and again refers to intrinsic properties of natural numbers:

Open Problem 2. *Is there an incongruent system with all moduli odd?*

In 1967, Selfridge [7] showed that if there exists a CS with no $n_i | n_j$ $(i \neq j)$, then the answer to the open problem is affirmative. BFF found also another result concerning this topic [2]:

Theorem 4. *If the moduli n_i are all odd, then $g(N) \geq 1$, where*

$$N = lcm(n_1, ..., n_k) = \prod_{j=1}^{m} p_j^{r_j}$$
$$x_j = \frac{\sum_{s=0}^{r_j - 1} p_j^s}{p_j^{r_j} - \sum_{s=0}^{r_j-1} p_j^s}$$
$$g(N) = \prod_{j=1}^{m} (1 + x_j) \ - \sum_{j=1}^{m} s_j \ - 1$$

We finish this section with a minor problem this time. Suppose $\mathcal{S}$ is incongruent, then it is not disjoint, so

$$1 = d(\bigcup_{i=1}^{k} \mathcal{A}_i) < \sum_{i=1}^{k} d(\mathcal{A}_i) = \sum_{i=1}^{k} n_i^{-1}$$

The problem is to evaluate the last sum. Is it true that $\sum n_i^{-1} \to \infty$ as $n_1 \to \infty$? If so, how fast is the divergence? If an integer m divides every modulus, what estimate can we do about $\sum n_i^{-1}$?

3.2. **Minimal Coverings.** These systems are those which covers the integers, but that no proper subsystem does. The most trivial ones are the disjoint coverings. Znam [13] showed that if $\mathcal{S}$ is disjoint, then $k \geq f(N)$ and there is infinitely many coverings for which equality holds. BFF once more extended this result [2]

Theorem 5. *If $\mathcal{S}$ is minimal, then $k \geq f(N)$ where*

$$f(N) = \sum_{j=1}^{m} r_j(p_j - 1) \ + 1$$

3.3. **Covering Function.** There are two ways of approaching covering systems. One can study unions of arithmetic sequences or one can take one integer at a time and see in which class of the covering in consideration it goes in. In the previous section, we used more of the first paradigm, but now we investigate the other option, although this path have not yet been investigated much.

Given a covering $\mathcal{S}$, we have seen that remodulising (mod N), we get all of [0,N-1] in $\mathbb{Z}/N\mathbb{Z}$, hence if $\mathcal{S}$ covers $N-1$ consecutive numbers, it covers $\mathbb{Z}$ entirely. P. Erdös once conjecture a stronger statement: if $\mathcal{S}$ covers 2^k consecutive integers (recall that k is the number of classes in $\mathcal{S}$), then it covers all integers. This result was proved later on by Selfridge and also by Crittenden and Vanden Eyden in 1970 [7]. This bound is best possible since the system $\{2^{i-1} \pmod{2^i}\}_{1\leq i\leq k}$ covers the 2^k-1 first integers, but not 2^k, hence not $\mathbb{Z}$.

We want to consider not only consecutive integers, but any integers. We introduce the following concept that permits us to do so:

Definition 3. The covering function $\mathcal{T}_{\mathcal{S}}:\mathbb{Z}\to\mathbb{Z}$ of a system $\mathcal{S}$ is defined as $\mathcal{T}_{\mathcal{S}}(m) =$ the number of classes containing m.

Znam [13] proved that if $\mathcal{S},\mathcal{S}'$ are incongruent and $\mathcal{T}_{\mathcal{S}}=\mathcal{T}_{\mathcal{S}'}$, then $\mathcal{S}=\mathcal{S}'$. Again BFF have generalised this theorem [2]:

Theorem 6. *Let $\mathcal{S}$, $\mathcal{S}'$ each have multiplicity less than p(N), then*

$$\mathcal{T}_{\mathcal{S}}=\mathcal{T}_{\mathcal{S}'}\Rightarrow\mathcal{S}=\mathcal{S}'$$

Finally we note another very interesting result from BFF. Remember that Theorem 1 of BFF was an extension of the Znam-Newman result. BFF did a different generalisation of the same theorem, with a completely new flavour, for it uses the covering function approache rather than the arithmetic sequence one.

Theorem 7. *If $\mathcal{T}_{\mathcal{S}}$ is constant (mod M), then each maximal modulus n has multiplicity at least* $\min(p(n),M)$.

Remark 3. If $\mathcal{S}$ is disjoint, then $\mathcal{T}_{\mathcal{S}}\equiv 1$, so theorem 1 follows from this one.

4. From Here

The topic of covering congruences is still somewhat not understood at great extent. There were a flow of results in the late 80's given by BFF using their new approach, and that was really a revolution in the topic, but even then, we do not know much. There are a ton of questions unanswered[7]; a few were given in this survey. And the various results we have seen seems sometimes to be sparse and useless. Some constructions were done using coverings; for exemple, Graham [8] showed that there exists an infinite Lucas sequence, that is $a_{n+2}=a_{n+1}+a_n$, $(a_0,a_1)=1$, such that no term is prime. Romanoff's problem and related problems are also linked to covering congruences. But the list of applications of CS is not extensive.

There are also generalisation to the concept of covering congruences that are studied [7]. We can look at systems of arithmetic sequence were the constants and the moduli are any positive real number. The most famous one is the Beatty sequence. A few results can be translated to such systems, for exemple in the Beatty sequence, the "classes" are disjoint and it is true that the sum of the inverse of the moduli is 1, as with DCS. This is clear since nowhere in the proof we used the fact that the moduli were integers.

It is also possible to extend CS to include infinite systems of congruences, but here the situation is not completely satisfactory, since there are several ways of defining such systems. To begin with, we can say that an infinite system $\mathcal{S} = \{a_i \pmod{n_i}\}$ is covering if every integer satisfies at least one of them and the density of integers not satisfying the first k tends to 0 as $k \to \infty$. Another possibility is $\mathcal{S}$ is covering if every (large) integer is of the form $a_i + tn_i$, where $t \geq 1$ is fixed. Finally, denote by f(k) the number of integers $m < n_k$ not satisfying the first k congruences, then $\mathcal{S}$ is covering if $\frac{f(k)}{k} \to 0$ as $k \to \infty$. All of these definitions bring their own questions and a different concept to infinite coverings. Which of the three is better? None for now. None has any interesting results and none has been enough understood to answer the question.

References

[1] Berger M.A., Felzenbaum A. and Fraenkel A.S., *A non-analytic proof of the Newman-Znam result for disjoint covering systems*, Combinatorica 6 (1986), pp.235–243

[2] —, *New results for covering systems of residue sets*, Bull.Amer.Math.Soc.(N.S.) 14, (1986), pp.121–125

[3] —, *Disjoint covering systems with precisely one multiple modulus*, Acta.Arith. L(1988), pp.171–182

[4] Choi S.L.G., *Covering the set of integers by congruence classes of distinct moduli* Math. Comp. 25 (1971), pp.885–895

[5] Erdös, P. *On integers of the form $2^n + p$ and some related problems.* Summa Brasil Math. 11 (1950), pp. 1–11

[6] — *On a problem concerning covering systems*(Hungarian, English summary), Mat.Lapok 3 (1952), pp. 122–128

[7] Erdös P. and Graham R.L., *Old and new problems and results in combinatorial number theory*, Monographie No.28 de L'enseignement Mathemtique, Universite de Geneve, 1980

[8] Graham, R.L., *A Fibonacci-like sequence of composite numbers* Math. Mag. 37 (1964), pp.322–324

[9] Newman, M. *Roots of unity and covering sets*, Math. Ann. 191 (1971), pp.279–282

[10] Porubsky S., *Generalization of some results for exactly covering systems*, Mat. Casopis Sloven. Akad. Vied 22 (1972), pp.208–214

[11] Simpson J. and Zeleke M., *Disjoint covering systems with precisly one repeated modulus*, Adv. Applied Math. 23 (1999), pp.322–332

[12] Stein S.K., *Unions of arithmetic sequences*, Math. Ann. 134 (1958), pp.289–294

[13] Znam, S. *On properties of systems of arithmetic sequences*, Acta Arith. 26 (1975), pp.279–283

[14] —, *On exacly covering systems of arithmetic sequences*, Math. Ann. 180 (1969),pp.227–232