

INFINITE COVERING SYSTEMS OF CONGRUENCES WHICH DON'T EXIST

ETHAN LEWIS

(Communicated by William W. Adams)

ABSTRACT. We prove there is no infinite set of congruences with: every integer satisfying exactly one congruence, distinct moduli, the sum of the reciprocals of the moduli equal to 1, the lcm of the moduli divisible by only finitely many primes, and a prime greater than 3 dividing any of the moduli.

1. INTRODUCTION

Recall that a covering system is a set of congruences such that every integer satisfies at least one congruence in the set. A disjoint (also called exact) covering system (DCS) is a covering system where each integer satisfies exactly one member of the set. A simple example is $\{x \equiv 0 \pmod{2}, x \equiv 1 \pmod{2}\}$. An incongruent (also called distinct) covering system is a covering system where all the moduli are different. An example is $\{x \equiv 0 \pmod{2}, x \equiv 0 \pmod{3}, x \equiv 1 \pmod{4}, x \equiv 1 \pmod{6}, x \equiv 11 \pmod{12}\}$. Two good general references are Porubský [9] and Berger, Felzenbaum and Fraenkel [2]. Guy in [5] gives a list of open problems in covering systems.

Recently there has been interest in problems dealing with DCS (see, for example, Simpson [12], Zeilberger [16] and Simpson and Zeilberger [13]) and in particular in problems of Infinite Incongruent Disjoint Covering Systems (IIDCS) (see Beebe [1], Berger, Felzenbaum, Fraenkel and Holzman [3], Fraenkel and Simpson [4], and Vanden Eynden [15]). An IIDCS is an infinite set of congruences, such that every integer satisfies at least one congruence in the set, with the incongruent and disjoint properties. It is well known (see [2] or [9]) that a finite covering system can not be both disjoint and incongruent. For an IIDCS a further requirement is usually added: that the sum of the reciprocals of the moduli equals one. In this case we call the system saturated, a property that is assumed in this paper. An example of an IIDCS is $\{x \equiv 0 \pmod{2}, x \equiv 1 \pmod{4}, x \equiv -1 \pmod{8}, \dots\}$ (the residues alternate taking the residue closest to 0 which has not been previously covered).

In 1958 Stein [14] asked if there were IIDCS's which used moduli other than $\{2^i : i > 0\}$. Krukenberg answered this question in his doctoral thesis [7]. In it he classifies IIDCS's with moduli of the form $2^i 3^j$. An example of one such IIDCS is:

Received by the editors December 9, 1992 and, in revised form, April 18, 1994 and August 20, 1994.

1991 *Mathematics Subject Classification*. Primary 11B25; Secondary 11A07.
Supported in part by DOE grant P200A20337.

cover the integers in the two smallest residues, $\{0, 1\}$, modulo 3 with $x \equiv 0 \pmod{3}$ and the collection of congruences obtained from the solution of $x \equiv 1 \pmod{3}$ with each member of the IIDCS above. Next, cover integers satisfying the two smallest remaining residues modulo 9 with $x \equiv 2 \pmod{9}$ and the collection of congruences obtained from the solution of $x \equiv 5 \pmod{9}$ with each member of the IIDCS above. Repeating this procedure indefinitely gives an IIDCS.

Still remaining is the question whether there are systems whose moduli are divisible by primes other than 2 and 3. In this paper we show that no such system exists unless an infinite number of distinct primes are used as divisors of the moduli. Combined with Krukenberg's result this completely classifies IIDCS's.

2. A TEST FOR THE EXISTENCE OF IIDCS'S

We start with definitions.

Definition of density and the function S . Let C be a collection of arithmetic progressions (AP's). Define $S(C)$ to be the set of integers in C , and $S_n(C)$ to be $S(C) \cap [1, \dots, n]$. Define the lower density, $\underline{\mathbf{d}}$, and the upper density, $\overline{\mathbf{d}}$, of C by

$$\begin{aligned}\underline{\mathbf{d}}(C) &= \liminf_{n \rightarrow \infty} |S_n(C)|/n, \\ \overline{\mathbf{d}}(C) &= \limsup_{n \rightarrow \infty} |S_n(C)|/n.\end{aligned}$$

If these are equal, then define the density of C by

$$\mathbf{d}(C) = \lim_{n \rightarrow \infty} |S_n(C)|/n.$$

Definition of division minimal. Let M be a set of integers. An element $m \in M$ is *division minimal* if there are no proper divisors of m in M .

The following is a theorem of C. A. Rogers in Chapter 5.3 of [6].

Theorem 1. Let $C = \{a_1 \pmod{m_1}, a_2 \pmod{m_2}, \dots, a_k \pmod{m_k}\}$ be a set of AP's and let $C' = \{0 \pmod{m_1}, 0 \pmod{m_2}, \dots, 0 \pmod{m_k}\}$. Then

$$\mathbf{d}(C) \geq \mathbf{d}(C').$$

Corollary 2.1. Let C be a finite collection of AP's. Let M be the set of its moduli. Then

$$\mathbf{d}(C) \geq \sum_{r \geq 1} \sum_{M_r} (-1)^{r+1} / \text{lcm}(M_r),$$

where M_r runs through all r -subsets of M .

Proof. Let C' be as in Theorem 1. Clearly

$$\mathbf{d}(C) \geq \mathbf{d}(C') = \sum_{M_r} (-1)^{r+1} / \text{lcm}(M_r),$$

where M_r runs through all r -subsets of M . The last equality is a consequence of the Chinese Remainder Theorem (see e.g. Theorem 13.6 in [8]). \square

We obtain more results about the density.

Lemma 2.1. *Let D be a saturated DCS and let $C \subset D$. Then*

$$\bar{\mathbf{d}}(C) + \underline{\mathbf{d}}(D \setminus C) = 1.$$

Proof. First note that since D is a DCS we have

$$\frac{S_n(D)}{n} = \frac{S_n(C)}{n} + \frac{S_n(D \setminus C)}{n} = 1$$

for all n . On p. 38 of [10] we have that for sequences $\{x_n\}$ and $\{y_n\}$ of real numbers

$$\liminf_{n \rightarrow \infty} (x_n + y_n) \leq \limsup_{n \rightarrow \infty} (x_n) + \liminf_{n \rightarrow \infty} (y_n) \leq \limsup_{n \rightarrow \infty} (x_n + y_n).$$

Letting

$$x_n = \frac{S_n(C)}{n} \quad \text{and} \quad y_n = \frac{S_n(D \setminus C)}{n}$$

we are done. \square

Lemma 2.2. *Let D be a saturated DCS and $C = \{c_i\} \subset D$. Then $\mathbf{d}(C)$ is well defined and*

$$\mathbf{d}(C) = \sum \mathbf{d}(c_i).$$

Proof. Let $D \setminus C = \{b_i\}$. Using Lemma 2.1 and the definition of saturated we have

$$1 = \bar{\mathbf{d}}(C) + \underline{\mathbf{d}}(D \setminus C) = \sum \mathbf{d}(c_i) + \sum \mathbf{d}(b_i),$$

hence

$$(1) \quad (\bar{\mathbf{d}}(C) - \sum \mathbf{d}(c_i)) + (\underline{\mathbf{d}}(D \setminus C) - \sum \mathbf{d}(b_i)) = 0.$$

Now note that $\underline{\mathbf{d}}(\bigcup_{i=1}^{\infty} b_i) \geq \underline{\mathbf{d}}(\bigcup_{i=1}^N b_i) = \sum_{i=1}^N \mathbf{d}(b_i)$. Letting $N \rightarrow \infty$ we have $\underline{\mathbf{d}}(D \setminus C) \geq \sum \mathbf{d}(b_i)$. Likewise for C we have $\bar{\mathbf{d}}(C) \geq \underline{\mathbf{d}}(C) \geq \sum \mathbf{d}(c_i)$. These inequalities and (1) imply $\underline{\mathbf{d}}(D \setminus C) = \sum \mathbf{d}(b_i)$ and $\bar{\mathbf{d}}(C) = \underline{\mathbf{d}}(C) = \sum \mathbf{d}(c_i)$, so we are done. \square

Next we present a consequence of the disjoint condition.

Lemma 2.3 (after Krukenberg [7]). *Let D be a disjoint system of congruences with*

$$x \equiv a \pmod{p^e N}, \quad p \text{ a prime, } p \nmid N$$

a member of D . If $x \equiv b \pmod{m}$ appears in D and has common solutions with

$$x \equiv a \pmod{p^{e-1} N},$$

then $p^e \mid m$.

Proof. Since D is a disjoint system, the residue classes $a \pmod{p^e N}$ and $b \pmod{m}$ are disjoint, so by the Chinese Remainder Theorem

$$\gcd(p^e N, m) \nmid a - b.$$

On the other hand the classes $a \pmod{p^{e-1} N}$ and $b \pmod{m}$ intersect, so by the Chinese Remainder Theorem

$$\gcd(p^{e-1} N, m) \mid a - b.$$

Thus $\gcd(p^e N, m) \neq \gcd(p^{e-1} N, m)$, which implies $p^e \mid m$. \square

Lemma 2.4. *Let M be a set of integers such that the cardinality of the set $P = \{p : p \mid m, m \in M \text{ and } p \text{ prime}\}$ is finite. Let M' be the set of division minimal elements in M . Then M' is finite.*

(This lemma appeared as problem 10350 in the American Mathematical Monthly **100** (1993), p. 952.)

Proof. Assume M' is infinite. Let $P = \{p_1, p_2, \dots, p_k\}$. For $m_i \in M'$ set $m_i = p_1^{e_1(i)} p_2^{e_2(i)} \dots p_k^{e_k(i)}$. Given $m_i \in M'$ there is an r such that $e_r(j) < e_r(i)$ for each $m_j \in M', j \neq i$, since otherwise m_i divides m_j . Since M' is infinite and the number of primes is finite, by the pigeon-hole principle there is a particular r_1 such that $e_{r_1}(j) < e_{r_1}(i)$ for infinitely many $m_j \in M'$. Thus there is some $f_1 < e_{r_1}(i)$ so that $e_{r_1}(j) = f_1$ for infinitely many $m_j \in M'$. Let the set $M_1 = \{m_j : m_j \in M', e_{r_1}(j) = f_1\}$. For $m_i \in M_1$ we can repeat the analysis above to show there is an $r_2 \neq r_1$ and an f_2 such that $e_{r_2}(j) = f_2$ for infinitely many $m_j \in M_1$. Repeating this construction k times we obtain that $M_k = \{m\}$ where $m = p_{r_1}^{f_{r_1}} p_{r_2}^{f_{r_2}} \dots p_{r_k}^{f_{r_k}}$ and that M_k is infinite, a contradiction. \square

We are ready for the main result.

Theorem 2. *Let $p_1 < p_2 < \dots < p_k$ be the set of primes used in an infinite, incongruent, disjoint and saturated covering system. Then*

$$\prod_{i=1}^k \frac{p_i}{p_i - 1} \geq p_k.$$

Proof. Let A be the set of moduli in the IIDCS which are divisible by p_k . Let M be the division minimal members of A , and let M' be $\{m/p_k : m \in M\}$. Let D be the set of AP's corresponding to A and let D' be the set of AP's corresponding to M . Construct a set of AP's, C , by dividing the modulus of each $d_i \in D'$ by p_k . We will obtain upper and lower bounds on $\mathbf{d}(D)$. By Lemma 2.3 we have that every integer in every AP in C must appear in some AP in D . Therefore $S(D) \supset S(C)$. By Lemma 2.4, $|C|$ is finite so we can apply Corollary 2.1. Thus

$$(2) \quad \mathbf{d}(D) \geq \mathbf{d}(C) \geq \sum_r \sum_{M_r} (-1)^{r+1} / \text{lcm}(M'_r) = p_k \sum_r \sum_{M_r} (-1)^{r+1} / \text{lcm}(M_r),$$

where M'_r and M_r run through all the r -subsets of M' and M respectively. For $m_i \in M$ define an infinite set of multiples of m_i by $N_i = \{n : n = m_i p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, e_1, e_2, \dots, e_k \geq 0\}$ and let $N = \bigcup N_i$. Thus $N \supset A$. Now let $N' = \bigcap_{i=1}^k N_{x_i}$ and let $M^* = \text{lcm}(m_{x_1}, m_{x_2}, \dots, m_{x_z})$. Clearly

$$(3) \quad \sum_{n \in N'} \frac{1}{n} = \frac{1}{M^*} \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \dots\right) \dots \left(1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \dots\right).$$

By Lemma 2.2 and the principle of inclusion-exclusion we have

$$(4) \quad \mathbf{d}(D) = \sum_{a \in A} \frac{1}{a} \leq \sum_{n \in N} \frac{1}{n} = \sum_r \sum_{M_r} \frac{(-1)^{r+1} (\prod_{i=1}^k p_i / (p_i - 1))}{\text{lcm}(M_r)},$$

where M_r run through all the r -subsets of M . Combining inequalities (2) and (4) and cancelling like terms proves the theorem. \square

Corollary 2.2. *If p_k is the greatest prime used in an IIDCS, then $p_k = 2$ or 3 .*

Proof. We want to show the inequality of Theorem 2 is false when $p_k > 3$. Rewriting the right side we have

$$\prod_{i=1}^k \frac{p_i}{p_i - 1} \geq \prod_{n=2}^{p_k} \frac{n}{n-1}.$$

It is clear that this inequality holds only when the set of primes used in the IIDCS is $\{2\}$ or $\{2,3\}$. \square

Corollary 2.3. *In a finite incongruent DCS the same arguments hold. Noting that A is now finite the inequality in (4) is now strict. Hence we obtain that $\prod_{i=1}^k p_i/(p_i - 1) > p_k$. Thus we have another proof of the nonexistence of finite incongruent DCS's.*

Corollary 2.4. *In a (finite) DCS let R be the maximum multiplicity of any modulus. Repeating the arguments above we obtain*

$$R \prod_{i=1}^k \frac{p_i}{p_i - 1} > p_k.$$

A stronger version of this result was obtained by Simpson in [12].

Remark. Let $M = \{m_i\}$ be the moduli used in an ICS and m_1 be the smallest member of M . Erdős conjectures that for ICS's

$$\sum_{m_i \in M} 1/m_i \rightarrow \infty \text{ as } m_1 \rightarrow \infty.$$

Since all known IIDCS's to date are convertible to ICS's with $\sum_{m \in M} 1/m$ arbitrarily close to 1 (see [9]), it seems Corollary 2.2 is a necessary condition for Erdős' conjecture to be true.

ACKNOWLEDGMENT

I would like to thank Jamie Simpson for his suggestions, and for pointing out Corollary 2.3. I would like to thank Herb Wilf for the great deal of help he gave me in rewriting this paper. I would like to thank Doron Zeilberger for introducing me to this area and for his enthusiastic support. I would like to thank Andrew Granville for his comments about the presentation. I also wish to thank Aviezri Fraenkel.

REFERENCES

1. J. Beebe, *Examples of infinite, incongruent exact covers*, Amer. Math. Monthly **95** (1988). MR **89g**:11013
2. M. A. Berger, A. Felzenbaum, and A. S. Fraenkel, *New results for covering systems of residue sets*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), 121–125. MR **87c**:11013
3. M. A. Berger, A. Felzenbaum, A. S. Fraenkel, and R. Holzman, *On infinite and finite covering systems*, Amer. Math. Monthly **98** (1991), 739–742. MR **92g**:11009
4. A. S. Fraenkel and R. J. Simpson, *On infinite disjoint covering systems*, Proc. Amer. Math. Soc. **119** (1993), 5–9. MR **93k**:11006
5. R. K. Guy, *Unsolved problems in number theory*, Springer, New York, 1981. MR **83k**:10002

6. H. Halberstam and K. F. Roth, *Sequences*, Springer, New York, 1983. MR **83m**:10094
7. C. E. Krukenberg, *Covering sets of the integers*, Ph.D. Thesis, Univ. of Illinois Urbana-Champaign, 1971.
8. W. J. Leveque, *Fundamentals of number theory*, Addison-Wesley, Reading, MA, 1977. MR **58**:465
9. Š. Porubský, *Results and problems on covering systems of residue classes*, Mitteilungen aus dem Math. Sem. Giessen, Heft 150, Universität Giessen, 1981. MR **83b**:10068
10. H. L. Royden, *Real analysis*, Macmillan, New York, 1988. MR **90g**:00004
11. R. J. Simpson, *Exact coverings of the integers by arithmetic progressions*, Discrete Math. **59** (1986), 181–190. MR **87f**:11011
12. ———, *Disjoint covering systems of congruences*, Amer. Math. Monthly **94** (1987), 865–868. MR **89b**:11006
13. R. J. Simpson and D. Zeilberger, *Necessary conditions for distinct covering systems with square-free moduli*, Acta Arith. **59** (1991), 59–70. MR **92i**:11014
14. S. K. Stein, *Unions of arithmetic sequences*, Math Ann. **134** (1958) 282–294. MR **20**:17
15. C. Vanden Eynden, *On a problem of Stein concerning infinite covers*, Amer. Math. Monthly **99** (1992), 355–358. MR **93b**:11004
16. D. Zeilberger, *On a conjecture of R. J. Simpson about exact covering congruences*, Amer. Math. Monthly **96** (1989), 243. MR **90a**:11008

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PENNSYLVANIA
19104-6395

E-mail address: ethan@thales.math.upenn.edu