Chapter 5

On A Conjecture Of Erdös

Proceedings—NCUR VIII. (1994), Vol. II, pp. 794–798.

Jeffrey F. Gold

Department of Mathematics, Department of Physics
University of Utah

Don H. Tucker

Department of Mathematics
University of Utah

In this paper we present some preliminary results on a conjecture by Paul Erdös [1,2,5] concerning covering sets of congruences. A covering set consists of a finite system of congruences with distinct moduli, such that every integer satisfies as a minimum one of the congruences. An interesting consequence of this conjecture is the dependence of the solution on abundant numbers; an abundant number is an integer whose sum of its proper divisors exceeds the integer.

Complementary Sets

Definition 1 *If a and b are integers, then*

$$a \bmod b = \{a, a \pm b, a \pm 2b, \ldots\} .$$

Definition 2 *If a_1,a_2,...,a_n,$b \in \mathbb{Z}$, then*

$$[a_1, a_2, \ldots, a_n] \bmod b = \{a_1 \bmod b\} \cup \{a_2 \bmod b\} \cup \cdots \cup \{a_n \bmod b\} = \bigcup_{i=1}^{n} \{a_i \bmod b\} .$$

The Remodulization Theorem [3] states that if $a, b, c \in \mathbb{Z}$ and $c > 0$, then

$$a \bmod b = [a, a+b, \ldots, a+b(c-1)] \bmod cb \ .$$

If we use Definition 2, the complementary set of $\{a \ mod \ b\}$ is given by

$$\{a \bmod b\}^c = \mathbb{Z} \setminus \{a \bmod b\} = [0, 1, 2, \ldots, a-1, a+1, \ldots, b-1] \bmod b \ .$$

In this case, the complementary set consists of $b-1$ congruences *modulo* b. We will always refer to the size of a set and its complement with respect to a specific modulus. The following theorem and its proof is found in [4].

Theorem 1 *The complementary set of* $\left\{ \bigcup_{i=1}^{n} [a_{i,1}, \ldots, a_{i,\alpha_{b_i}}] \bmod b_i \right\}$, *where* $a_{i,j} \neq a_{i,k}$ *for* $j \neq k$, *and* $\alpha_{b_i} < b_i$, *and the* b_i *are pairwise relatively prime, contains exactly* $\prod_{i=1}^{n}(b_i - \alpha_{b_i})$ *congruences modulo* $\prod_{i=1}^{n} b_i$.

Covering Sets of Congruences

In Davenport [1], a problem has been proposed to construct a set of congruences with distinct moduli, such that every integer is contained in at least one of the congruences of the system. All moduli are ≥ 2, since *modulo* 1 constitutes its own complete residue system. An extension has been proposed by Erdös [5]: If given any integer $N \geq 1$, does there exist a finite covering set of congruences using only distinct moduli greater than N?

The following system represents a set of covering congruences for $N = 1$:

$$\begin{cases} x \equiv 0 \bmod 2 \\ x \equiv 0 \bmod 3 \\ x \equiv 1 \bmod 4 \\ x \equiv 1 \bmod 6 \\ x \equiv 11 \bmod 12 \end{cases}$$

Note that the moduli are all divisors of 12.

Using the remodulization method to remodulize each congruence to the modulus 12, we have

$$\begin{cases} x \equiv [0, 2, 4, 6, 8, 10] \bmod 12 \\ x \equiv [0, 3, 6, 9] \bmod 12 \\ x \equiv [1, 5, 9] \bmod 12 \\ x \equiv [1, 7] \bmod 12 \\ x \equiv [11] \bmod 12 \end{cases} \tag{5.1}$$

By inspection, this system constitutes a covering system, because it is equivalent to the complete residue system *modulo* 12, that is, $[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]$

$\mathrm{mod}12 \equiv \mathbb{Z}$.

The question naturally arises as to the possibility of constructing a set of covering congruences whose moduli are pairwise relatively prime. The answer is no, as we will now show. The proof depends on results of Theorem 1.

Theorem 2 *Any finite system of congruences* $\left\{\bigcup_{i=1}^{n}[a_{i,1}, a_{i,2}, \ldots, a_{i,\alpha_{b_i}}] \bmod b_i\right\}$, *where the* b_i *are pairwise relatively prime, and* $a_{i,k} \neq a_{i,m}$ *for* $k \neq m$, *and* $\alpha_{b_i} < b_i$, *cannot form a covering set of congruences.*

Proof. We use Theorem 1, for the case $\alpha_{b_i} = 1$ for $1 \leq i \leq n$. For a system of congruences $\{\bigcup_{i=1}^{n} a_i \bmod b_i\}$ with pairwise relatively prime moduli b_i to be a covering set, it is necessary that the system of congruences forms a complete residue system, that is, a union of $\prod_{i=1}^{n} b_i$ distinct (incongruent) residues *modulo* $\prod_{i=1}^{n} b_i$. However, since the complementary set consists of $\prod_{i=1}^{n}(b_i - 1)$ congruences *modulo* $\prod_{i=1}^{n} b_i$, the system consists of $\prod_{i=1}^{n} b_i - \prod_{i=1}^{n}(b_i - 1)$ congruences *modulo* $\prod_{i=1}^{n} b_i$. This means that $\prod_{i=1}^{n} b_i - \prod_{i=1}^{n}(b_i - 1)$ must equal $\prod_{i=1}^{n} b_i$, or $\prod_{i=1}^{n}(b_i - 1) = 0$; this is a contradiction, since $2 \leq b_1 < b_2 < \ldots < b_n$. That is to say, it takes infinitely many congruences with pairwise relatively prime moduli to construct a covering set.

The situation is actually much worse; if we construct a system of congruences

$$\left\{\bigcup_{i=1}^{n}[a_{i,1}, a_{i,2}, \ldots, a_{i,\alpha_{b_i}}] \bmod b_i\right\},$$

a system of congruences with α_{b_i} residues for each modulus b_i, where $\alpha_{b_i} < b_i$, and $a_{i,k} \neq a_{i,m}$ for $k \neq m$, then the complementary set consists of $\prod_{i=1}^{n}(b_i - \alpha_{b_i})$ congruences *modulo* $\prod_{i=1}^{n} b_i$. Here, $\prod_{i=1}^{n}(b_i - \alpha_{b_i})$ must equal zero, which is a contradiction because $b_i - \alpha_{b_i} \geq 1$. Again, it takes infinitely many such congruences to construct a covering set. In the extreme case, when $\alpha_{b_i} = b_i - 1$, we have the system

$$\left\{\begin{array}{rcl} x & \equiv & [a_{1,1}, a_{1,2}, \ldots, a_{1,b_1-1}] \bmod b_1 \\ x & \equiv & [a_{2,1}, a_{2,2}, \ldots, a_{2,b_2-1}] \bmod b_2 \\ & \vdots & \\ x & \equiv & [a_{n,1}, a_{n,2}, \ldots, a_{n,b_n-1}] \bmod b_n \end{array}\right. \tag{5.2}$$

where the b_i are pairwise relatively prime, and each set of congruences *modulo* b_i contains $b_i - 1$ congruences, i.e., one congruence shy of a complete residue system for each *modulus* b_i. The complement of the system consists of $\prod_{i=1}^{n}(b_i - (b_i - 1))$ congruence *modulo* $\prod_{i=1}^{n} b_i$, or 1 congruence *modulo* $\prod_{i=1}^{n} b_i$. Hence the system (5.2) contains a complete residue system only if we cap it off with the last

remaining residue *modulo* $\prod_{i=1}^{n} b_i$. However, by adding to the system the remaining congruence, we have relaxed our requirement that all the moduli are pairwise relatively prime.

Upshot If a finite system of distinct congruences (5.2) with pairwise relatively prime moduli forms a covering set, it must contain a congruence class which itself forms a complete residue system, or covering set.

Suppose p_1 is a prime such that $p_1 > N$, and $M = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, where $p_1 < p_2 < \ldots < p_n$. The total number of divisors of M which are $\leq M$ is $\prod_{i=1}^{n}(\lambda_i + 1)$; however, to form a covering set we may only use all factors greater than 1, the total number of useable factors is $\xi = -1 + \prod_{i=1}^{n}(\lambda_i + 1)$. We now construct a system of ξ congruences

$$\begin{cases} x \equiv c_1 \bmod d_1 \\ x \equiv c_2 \bmod d_2 \\ \qquad \vdots \\ x \equiv c_\xi \bmod d_\xi \end{cases} \tag{5.3}$$

where the d_i are the various factors of $M = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, and $d_1 < d_2 < \ldots < d_\xi$. Note that $d_1 = p_1$ and $d_\xi = M$.

Observation 1 *The number of congruences is given by*

$$\sum_{i=1}^{\xi} \frac{M}{d_i} = \frac{M}{d_1} + \frac{M}{d_2} + \cdots + \frac{M}{d_\xi} = 1 + d_1 + d_2 + \cdots + d_{\xi-1} = \sigma_0(M) \ ,$$

after remodulizing all congruences of system (5.3) to the modulus $M = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$. *Here,* σ_0 *denotes the sum of all proper divisors, i.e., all positive divisors less than* M.

Up to this point we have not made any claims about these residues *modulo* M, that is, we have not yet determined how many repetitions exist, and equivalently, if the total number of distinct residues is sufficient to create a complete residue system *modulo* M. We can see, however, that the total number of residues must be at least M to form a complete residue system *modulo* M. Therefore, M must be an abundant or perfect number, that is, the sum of all proper divisors

$$\sum_{i=1}^{\xi} \frac{M}{d_i} = 1 + d_1 + d_2 + \cdots + d_{\xi-1} = \sigma_0(M) \geq M$$

in order for this system to contain a complete residue system *modulo* M. We have proved the following theorem.

Theorem 3 *In order for the proper divisors of a number M to constitute the moduli of a covering set it is necessary that M be perfect or abundant, i.e., $\sigma_0(M) \geq M$.*

We will prove in Theorem 5 that if M is a perfect number, i.e., $\sigma_0(M) = M$, then a system (5.3) cannot comprise a covering set.

Observation 2 *It may not be necessary to use all divisors of an abundant number M to form a covering set; however, according to our enumeration of the residues modulo M of system (5.3), we must remove all residues associated with the divisors that are removed. For example, suppose we don't use the divisor d_k, then we must remove a total of M/d_k residues from the set of $\sigma_0(M)$ residues counted in Observation 1. However, the divisor d_k cannot contain the greatest multiple of any one prime appearing in the prime decomposition $M = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$, for in that case, $lcm(d_1, d_2, \ldots, d_{k-1}, d_{k+1}, \ldots, d_\xi) \neq M$, that is to say, we would not have remodulized the system to the modulus M, but instead to some modulus $< M$.*

In the original set

$$\begin{cases} x \equiv [0, 2, 4, 6, 8, 10] \bmod 12 \\ x \equiv [0, 3, 6, 9] \bmod 12 \\ x \equiv [1, 5, 9] \bmod 12 \\ x \equiv [1, 7] \bmod 12 \\ x \equiv [11] \bmod 12 \end{cases}$$

we find that the integers 0,1,6, and 9 represent 4 repetitions, since $\sigma_0(12) - 12 = 4$. The total number of repetitions that occur in a system (5.3) which forms a covering set is $\sigma_0(M) - M$. The following theorem enumerates the total number of repetitions that occur in two congruences.

Theorem 4 *If two congruences a_1 mod b_1 and a_2 mod b_2, where $gcd(b_1, b_2) = 1$, are remodulized to the modulus pb_1b_2, where $p \in \mathbb{Z}$, then the solution set (intersection) consists of p residues modulo pb_1b_2.*

Proof. If we obtain a pair of congruences

$$\begin{cases} x & \equiv & a_1 \bmod b_1 \\ x & \equiv & a_2 \bmod b_2 \end{cases} \tag{5.4}$$

where b_1 and b_2 are relatively prime, then remodulizing each to *modulo* b_1b_2, the intersection by the Chinese Remainder Theorem [3] is determined to be the unique congruence $x \equiv a_0$ *mod* b_1b_2, where $a_1 \leq a_0 \leq a_1 + b_1(b_2 - 1)$ and $a_2 \leq a_0 \leq a_2 + b_2(b_1 - 1)$. If the pair is remodulized, not to the smallest modulus,

b_1b_2, but instead to some multiple of it, say pb_1b_2, where p is a positive integer, then

$$\begin{cases} x & \equiv & [a_1, a_1+b_1, \ldots, a_1+b_1(pb_2-1)] \bmod pb_1b_2 \\ x & \equiv & [a_2, a_2+b_2, \ldots, a_2+b_2(pb_1-1)] \bmod pb_1b_2 \end{cases} \tag{5.5}$$

We show that the intersection of (5.5) is

$$[a_0, a_0+b_1b_2, \ldots, a_0+b_1b_2(p-1)] \bmod pb_1b_2 \ ,$$

which is equivalent to the solution a_0 *mod* b_1b_2 of the original pair after a_0 *mod* b_1b_2 has been remodulized by the factor p. By writing the first congruence of (5.5) as

$$\begin{array}{lllll} a_1 \bmod b_1 = [& a_1, & a_1+b_1, & \ldots & a_1+b_1(b_2-1), \\ & a_1+b_1b_2, & a_1+b_1+b_1b_2, & \ldots & a_1+b_1(2b_2-1), \\ & \vdots & \vdots & & \vdots \\ & a_1+(p-1)b_1b_2, & a_1+b_1+(p-1)b_1b_2, & \ldots & a_1+b_1(pb_2-1)] \ mod\ pb_1b_2 \end{array}$$

we note that the first row contains the solution, a_0 *mod* pb_1b_2. Moreover, by adding multiples of b_1b_2 to the residue a_0, we find the subsequent solutions within the same column; hence there are p solutions (*modulo* pb_1b_2). Constructing the second congruence of (5.5) in the same manner, we extract the same p solutions. Therefore, if a pair of congruences (5.4) is remodulized to the modulus pb_1b_2, then they share exactly p simultaneous residues.

As an example, if we have the pair of congruences

$$\begin{cases} x \equiv a_1 \bmod p_1 \\ x \equiv a_2 \bmod p_2 \end{cases}$$

which are remodulized to the modulus $M = p_1^{\lambda_1}p_2^{\lambda_2}\cdots p_n^{\lambda_n}$, then they share

$$M/p_1p_2 = p_1^{(\lambda_1-1)}p_2^{(\lambda_2-1)}p_3^{\lambda_3}\cdots p_n^{\lambda_n}$$

residues *modulo* M.

Theorem 5 *If M is a perfect number, then a system of congruences whose moduli consist of all divisors > 1 of M cannot form a covering set.*

Proof. Suppose M is an even perfect number [6]; then it is of the form 2^kp, where p is an odd prime of the form $2^{k+1}-1$. Suppose we form a system of congruences (5.3) where the d_i are all divisors of M greater than 1, and remodulize all congruences *modulo* d_i to the modulus M. By Observation 1, $\sigma_0(M) = M$; a complete residue system *modulo* M must contain M distinct residues *modulo* M. Since p is prime, the congruences modulo 2 and modulo p

share 1 residue *modulo* $2p$, or 2^{k-1} residues *modulo* $2^k p$ by Theorem 4. These represent 2^{k-1} repetitions, and $M - 2^{k-1} < M = \sigma_0(M)$; hence the total number of distinct residues is not sufficient to form a covering set.

If M is an odd perfect number (if any exist), then it must contain more than 8 distinct prime factors [7]. Since p_1 and p_2 are two distinct prime factors, their intersection contains 1 congruence *modulo* $p_1 p_2$, or $M/p_1 p_2$ congruences *modulo* M. In that case, $M - M/p_1 p_2 < M = \sigma_0(M)$, meaning that the total number of distinct residues *modulo* M is too small for a system of congruences (5.3) to form a covering set.

Remark 1 *Theorems 3 and 5 combined suggest that if for each $N \geq 2$ there exists a covering set whose distinct moduli all exceed N, then there would exist abundant numbers whose least prime factor exceeds N. This is true. In fact, even more is true.*

Definition 3 *A number M is said to be abundant of order $k \geq 1$ if and only if $\sigma_0(M)/M > k$.*

Theorem 6 *If K and N are any integers, then there exists an integer M, abundant of order K, whose least prime factor exceeds N.*

Proof. Since the primes are such that $\sum 1/p_i = +\infty$, we may select $N < p_1 < p_2 < \cdots < p_n$ such that $\sum_{i=1}^{n} 1/p_i = K$. Set $M = \prod_{i=1}^{n} p_i$, then $\sigma_0(M) = 1 + p_1 + p_2 + \cdots + p_1 p_2 \cdots p_{n-1}$ and $\sigma_0(M)/M = 1/(p_1 \cdots p_n) + 1/(p_2 \cdots p_n) + \cdots + 1/p_1 + \cdots + 1/p_n > K$.

Remark 2 *Theorem 6 shows that there are numbers M whose divisors cannot yet be excluded from forming a covering set whose moduli all exceed N. However, a settling of this conjecture may well require finding methods that can accurately account for the total number of repetitions that occur in such systems.*

References

[1] Harold Davenport, *The Higher Arithmetic*, Dover Publications, Inc., New York, 1983. p. 57.

[2] Erdös, Paul, *On Integers of the Form $2^k + p$ and some Related Problems*, Summa Brasiliensis Mathematicae, Instituto de Mathematica Pura e Aplicada, 1950, Vol. 2, p. 120.

[3] Gold, Jeffrey F. and Don H. Tucker, *Remodulization of Congruences*, Proceedings — National Conference on Undergraduate Research, (University of

North Carolina Press, Asheville, North Carolina, 1992), Vol. II, pp. 1036–41.

[4] Gold, Jeffrey F. and Don H. Tucker, *Complementary Sets of Systems of Congruences*, Proceedings — National Conference on Undergraduate Research, (University of North Carolina Press, Asheville, North Carolina, 1993), Vol. II, pp. 793–96.

[5] Wacław Sierpiński, *Elementary Theory of Numbers*, Państwowe Wydawnictwo Naukowe, Warszawa, 1964, pp. 190, 413.

[6] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, Third Edition, Addison-Wesley Publishing Company, Massachusetts, 1993, pp. 223–29.

[7] David M. Burton, *Elementary Number Theory*, Second Edition, Wm. C. Brown Publishers, Iowa, 1989, p. 167.