ANY \( n \) ARITHMETIC PROGRESSIONS COVERING THE FIRST \( 2^n \) INTEGERS COVER ALL INTEGERS

R. B. CRITTENDEN AND C. L. VANDEN EYNDEN

In 1958 S. Stein [7] defined a system of \( n \) congruences \( x = a_i \pmod{b_i}, 1 \leq i \leq n \), to be disjoint if no \( x \) satisfies more than one of them. He conjectured that for every disjoint system of \( n \) congruences with distinct moduli there exists an \( x, 1 \leq x \leq 2^n \), satisfying none of them. P. Erdős [2] proved this with \( n2^n \) instead of \( 2^n \) and proposed the stronger conjecture that any system of \( n \) congruence classes not covering all integers omits some \( x \) between 1 and \( 2^n \). He proved this with \( 2^n \) replaced by some constant depending only on \( n \).

Erdős repeated both conjectures at the number theory conferences in Boulder, Colorado [3], and Pasadena, California [4], in 1963. Prizes of $10 and $25 were announced at the former for their solution.

The first conjecture was proved by J. Selfridge [6]. In this paper we prove the second conjecture [1]. That \( 2^n \) is the best possible follows from the example \( x \equiv 2^{i-1} \pmod{2^i}, 1 \leq i \leq n \), which covers 1, 2, \ldots, \( 2^n - 1 \).

The content of our Lemma 1 was discovered independently by J. Selfridge [5], who has also proved this conjecture.

**Theorem.** Let \( a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \) be given, the \( b \)'s positive. Suppose there exists an integer \( x_0 \) satisfying none of the congruences

\[
x \equiv a_i \pmod{b_i}, \quad i = 1, 2, \ldots, n.
\]

Then there is such an \( x_0 \) among 1, 2, 3, \ldots, \( 2^n \).

**Lemma 1.** Suppose the above theorem is false. Then for some \( n \) there exist congruences

\[
x \equiv a_i \pmod{b_i}, \quad i = 1, 2, \ldots, n
\]

such that the following three conditions all hold:

(A) If \( 1 \leq x \leq 2^n \), then \( x \) satisfies at least one of the congruences; but 0 satisfies none of them.

(B) All the \( b \)'s are prime.

(C) If \( k \) of the congruences have the prime modulus \( p \), then \( 2^k < p \).

Received by the editors March 24, 1969.

1 Partially supported by NSF grants GP 6663 and GP 8075.
Proof. Let us assume \( n \) is the smallest positive integer for which the theorem fails. Then there exist \( a_i \) and \( b_i, 1 \leq i \leq n \), such that each \( x \) from 1 to \( 2^n \) satisfies \( x \equiv a_i \pmod{b_i} \) for some \( i \), yet if \( T = \{x: x \not\equiv a_i \pmod{b_i}, 1 \leq i \leq n\} \), then \( T \) is nonempty. Clearly if \( x \in T \) and \( x \equiv x' \pmod{\operatorname{LCM}(b_1, b_2, \ldots, b_n)} \), then \( x' \in T \); thus \( T \) contains negative numbers. Let \( x_0 \) be the greatest nonpositive element of \( T \). Then the congruences \( x \equiv a_i - x_0 \pmod{b_i}, i = 1, 2, \ldots, n \), satisfy condition (A).

Let us now suppose the congruences \( x \equiv a_i \pmod{b_i}, 1 \leq i \leq n \), satisfy (A). We will make a start on (B) by proving that we may assume all the moduli are prime powers. Suppose one of the congruences is \( x \equiv a \pmod{b} \), where \( b \) is not a prime power. If each prime power dividing \( b \) also divided \( a \), then we would have \( b \mid a \), in contradiction to the second condition of (A). Thus we may assume \( b = p^a q \), where \( p \) is prime \( q > 1 \), \( p \mid q \), and \( b \nmid a \). Then replacing the congruence \( x \equiv a \pmod{b} \) with \( x \equiv a \pmod{p^a} \) yields a new set of congruences for which (A) still holds. In fact, if \( p \mid a \) the replacement \( x \equiv a \pmod{p} \) works. (The condition \( p \mid a \) precludes 0 as a solution of the new congruence.) Continuing in this way, we see we can produce \( n \) congruences which satisfy (A), such that if \( x \equiv a \pmod{b} \) is one of them, then \( b = p^a, p \) prime, and \( p \mid a \) if \( \alpha > 1 \).

Assuming our \( n \) congruences are as just described, we will now show (C) must hold. Let \( p \) be a fixed prime, and suppose exactly \( k \) of our congruences have modulus \( p \). Since 0 is a solution of no congruence, no multiple of \( p \) is a solution of any of these \( k \) congruences. Thus the multiples of \( p \) between 1 and \( 2^n \) each must be a solution of at least one of the remaining \( n-k \) congruences. These all have modulus either \( p^\alpha \) with \( \alpha > 1 \) or else \( b \) where \( p \nmid b \). The solutions of the former are all multiples of \( p \) by the last paragraph. The latter we replace by the single congruence modulo \( pb \) that is equivalent to the pair of congruences \( x \equiv a \pmod{b} \) and \( x \equiv 0 \pmod{p} \), according to the Chinese remainder theorem. None of the multiples of \( p \) are lost as solutions by this replacement.

We now have \( n-k \) congruences, each of the form \( x \equiv ap \pmod{bp} \), which include among their solutions \( p, 2p, \ldots, \lceil 2^n/p \rceil p \), but not 0. Then the \( n-k \) congruences \( x \equiv a \pmod{b} \) have among their solutions \( 1, 2, \ldots, \lfloor 2^n/p \rfloor \), but still not 0. Recall we assumed \( n \) to be the least integer for which the theorem fails. The theorem must be true for \( n-k \), which implies that \( \lfloor 2^n/p \rfloor < 2^{n-k} \). Thus \( 2^n/p < 2^{n-k} \), or \( 2^k < p \). This is (C).

Now we return to (B). Suppose \( p \) is prime. By what has gone before we can assume we have congruences of three types

\( 1) \ x \equiv a \pmod{p}, \) where \( p \mid a \),
\[(2) \ x \equiv a \pmod{p^a}, \text{ where } \alpha > 1 \text{ and } p \mid a,\]

\[(3) \ x \equiv a \pmod{b}, \text{ where } p \mid b.\]

We may assume each \(a\) is positive and less than the corresponding modulus. Since \(2^{p-1} \geq p\) for \(p \geq 2\), (C) implies that there exists \(a_0, \ 1 \leq a_0 < p\), such that \(x \equiv a_0 \pmod{p}\) is not one of our congruences. Let \(M = \Pi b\), where \(b\) runs through the moduli prime to \(p\). Choose \(r\) such that \(rM = a_0 \pmod{p}\). We claim that \(rM\) is not a solution to any of the congruences. Our choice of \(r\) eliminates the type (1) and type (2) congruences. Type (3) is out because \(b \mid rM\) but 0 is not a solution to any congruence. Suppose now we replace each type (2) congruence \(x \equiv a \pmod{p^a}\) with \(x \equiv a \pmod{p}\). The integers 1, 2, \(\cdots\), \(2^n\) are still all solutions of some congruence; but now so is 0. We have lost (A). The integer \(rM\) is still not a solution, however, since only multiples of \(p\) have been added. Thus condition (A) can be restored by another shift, exactly as in the beginning of the proof of this lemma. Note that we have replaced the modulus \(p^a\) by \(p\). We continue in this way until all moduli are primes. Thus (B) can be assumed.

**Lemma 2.** Suppose that \(S_1, S_2, \cdots, S_t\) are sets of integers such that \(S_i\) consists exactly of \(k_i\) residue classes modulo \(b_i, i = 1, 2, \cdots, t,\) and that \((b_i, b_j) = 1\) if \(i \neq j\). Suppose \(n\) is a positive integer, and let \(N\) be the number of integers \(x, 1 \leq x \leq 2^n,\) such that \(x\) is in none of the \(S_i\)'s. Then if \(1 \leq s \leq t,\) we have

\[
N > 1 + 2^n \left(1 - \sum_{i=1}^{t} k_i/b_i\right) \prod_{i=s+1}^{t} (1 - k_i/b_i) \\
- \left(1 + \sum_{i=1}^{s} k_i\right) \prod_{i=s+1}^{t} (1 + k_i).
\]

**Proof.** For \(S\) any set, let \(C(S)\) be the characteristic function of \(S\). First we note that \(1 - \sum_{i=1}^{t} C(S_i) \leq \prod_{i=1}^{t} \left(1 - C(S_i)\right),\) since the right side is nonnegative and the left side is nonpositive unless \(C(S_i) = 0, i = 1, 2, \cdots, s,\) in which case both sides are 1. We see the characteristic function of the set of integers not in any \(S\) is

\[
C\left(\sim \bigcup_{i=1}^{t} S_i\right) = C\left(\bigcap_{i=1}^{t} \sim S_i\right) = \prod_{i=1}^{t} C(\sim S_i) = \prod_{i=1}^{t} (1 - C(S_i))
\]

\[
= \prod_{i=1}^{s} (1 - C(S_i)) \prod_{i=s+1}^{t} (1 - C(S_i))
\]

\[
\geq \left(1 - \sum_{i=1}^{s} C(S_i)\right) \prod_{i=s+1}^{t} (1 - C(S_i))
\]

\[
= 1 - \sum_{i=1}^{s} C(S_i) + \sum_{i<j} C(S_i \cap S_j) - \cdots,
\]
where $\sum'$ indicates that at most one subscript is $\leq s$.

There are $k_i$ elements of $S_i$ among any $b_i$ consecutive integers, so

$$[2^n/b_i]k_i \leq \sum_{r=1}^{2^n} C(S_i)(r) \leq [2^n/b_i]k_i + k_i.$$  

Since $[2^n/b_i]k_i \leq 2^n k_i / b_i < [2^n/b_i]k_i + k_i$, we have $\sum_{r=1}^{2^n} C(S_i)(r) = 2^n k_i / b_i + E_i$, where $|E_i| < k_i$. (Note that $E_i = 0$ if $b_i | 2^n$.) More generally, the Chinese remainder theorem implies that there are $k_ik_j \cdots k_z$ elements of $S_i \cap S_j \cap \cdots \cap S_z$ among any $b_i b_j \cdots b_z$ consecutive integers, so

$$\sum_{r=1}^{2^n} C(S_i \cap S_j \cap \cdots \cap S_z)(r) = 2^n k_i k_j \cdots k_z / b_i b_j \cdots b_z + E_{ij} \cdots z,$$

where $|E_{ij} \cdots z| < k_ik_j \cdots k_z$. Then

$$N = \sum_{r=1}^{2^n} C \left( \bigcup_{i=1}^{t} S_i \right)(r) \geq \sum_{r=1}^{2^n} \left( 1 - \sum_{i=1}^{\ell} C(S_i) + \sum' C(S_i \cap S_j) - \cdots \right)(r)$$

$$= 2^n - \sum_{i=1}^{\ell} 2^n k_i / b_i + \sum' 2^n k_i k_j / b_i b_j - \cdots + E$$

$$= 2^n \left( 1 - \sum_{i=1}^{\ell} k_i / b_i \right) \prod_{i=\ell+1}^{t} (1 - k_i / b_i) + E,$$

where

$$|E| = \left| \sum_{i=1}^{t} E_i - \sum' E_{ij} + \cdots \right|$$

$$< \sum_{i=1}^{t} k_i + \sum' k_i k_j + \cdots = \left( 1 + \sum_{i=1}^{t} k_i \right) \prod_{i=\ell+1}^{t} (1 + k_i) - 1.$$  

The lemma follows.

**Lemma 3.** Suppose $b$, $b'$, $r$, $r'$, $k$, and $k'$ are integers such that $0 < b \leq b'$, $0 \leq k < r$, $0 < k' \leq r'$, and $b - b' + r' \leq r$. Then there exists a positive integer $u$ such that $k + u \leq r$, $k' - u \geq 0$, and

$$(1 - k / b)(1 - k' / b') \geq (1 - (k + u) / b)(1 - (k' - u) / b').$$

**Proof.** For $u > 0$ the last inequality is easily seen to be equivalent to $u \geq b - k - b' + k'$. We define $u$ to be max $(1, b - k - b' + k')$, making
this relation automatic. If \( u = 1 \), the first two inequalities are trivial. Otherwise \( k + u = b - b' + k' \leq b - b' + r' \leq r \), while \( k' - u = b' - b + k \geq 0 \).

**Lemma 4.** If the theorem is false, then it fails for some \( n < 20 \).

**Proof.** Suppose not. Then there exists \( n \geq 20 \) and \( n \) congruences such that the conditions of Lemma 1 hold. Suppose \( k_i \) congruences have modulus \( p_i \), \( p_1 < p_2 < \cdots < p_t \). By Lemma 2 (applied to the last \( t - s \) rather than the first \( s \) factors) we will get a contradiction if we can show

\[
(*) \quad 2^n \left(1 - \sum_{i=s+1}^{t} \frac{k_i}{p_i}\right) \prod_{i=s+1}^{t} \left(1 - \frac{k_i}{p_i}\right) \geq \left(1 + \sum_{i=s+1}^{t} k_i\right) \prod_{i=1}^{t} \left(1 + k_i\right)
\]

for some \( s, 1 \leq s \leq t \). We shall take \( s = \min\left(\left\lceil n/3 \right\rceil - 1, t - 1\right) \). The right side of \((*)\) has \( s + 1 \) factors. Since \( n = \sum k_i \), their sum is \( n + s + 1 \). The expression is maximized when all the factors are equal. Thus

\[
\text{right side of (*)} \leq \left(\frac{n + s + 1}{s + 1}\right)^{s+1} \leq \left(\frac{n + n/3}{n/3}\right)^{n/3} = 4^{n/3}.
\]

Here we used that \((1+n/z)^z\) is an increasing function of \( z \).

It can be seen from inspecting a table of primes that \( \pi(n - \left\lceil n/3 \right\rceil + 1) \leq \left\lceil n/3 \right\rceil \) for small values of \( n \geq 20 \); for larger \( n \) it follows from known estimates for \( \pi(n) \). Thus if \( s = \left\lceil n/3 \right\rceil - 1 \), we have

\[
\sum_{i=s+1}^{t} k_i = n - \sum_{i=1}^{t} k_i \leq n - \left\lceil n/3 \right\rceil + 1 \leq (\text{the \left\lceil n/3 \right\rceil rd prime}) < p_{\left\lceil n/3 \right\rceil}.
\]

If we define \( k_0 = \sum_{i=\left\lceil n/3 \right\rceil}^{t} k_i \) and \( p_0 = p_{\left\lceil n/3 \right\rceil} \), we have

\[
(1) \quad (\text{left side of (*)}) \geq 2^n \prod_{i=0}^{t} \left(1 - \frac{k_i}{p_i}\right),
\]

where \( k_0 < p_0 \), and \( k_i \leq \left\lceil \log p_i \right\rceil \) for \( i = 1, 2, \cdots, s \) by condition \((C)\) of Lemma 1. If \( s = t - 1 \) defining \( p_0 = p_t \) and \( k_0 = k_t \) also gives \((1)\).

For convenience, we introduce a new notation. Let \( m_p = k_i \) if \( p = p_i \) and 0 otherwise. Then

\[
\prod_{i=0}^{t} \left(1 - \frac{k_i}{p_i}\right) = \prod_{p} \left(1 - \frac{m_p}{p}\right).
\]

Since \( \sum_{i} k_i \geq 20 \), the conditions \( k_0 < p_0 \) and \( k_i \leq \left\lceil \log p_i \right\rceil \) for \( i \geq 1 \) imply \( p_0 \geq 13 \). In particular, \( m_3 = 0, m_5 \leq 1, m_7 \leq 2, m_{11} \leq 3, \) and \( m_{13} \leq 12 \). If \( p_0 = 13 \), then \( n = 20 \) and

\[
\prod_{p} \left(1 - \frac{m_p}{p}\right) = (1 - 1/3)(1 - 2/5)(1 - 2/7)(1 - 3/11)(1 - 12/13).
\]
In this case

\[ 2^n \prod_p \left(1 - \frac{m_p}{p}\right) - 4^{n/3} = 2^{n/3} \prod_p \left(1 - \frac{m_p}{p}\right) - 1 \]

\[ = 2^{40/3} \left(\frac{2^{10/3} + 2/3}{1001} - 1\right) > 0, \]

which implies (\(*\)). Clearly \(2^{n/3} \prod_p (1 - m_p/p) > 1\) is sufficient to imply (\(*\)) in general. We will show that for \(n > 20\)

\[ \prod_p \left(1 - \frac{m_p}{p}\right) \]

\[ \geq (1 - 1/3)(1 - 2/5)(1 - 2/7)(1 - 3/11)(1 - 12/13)^{(n-8)/12}. \]

Then

\[ 2^{n/3} \prod_p \left(1 - \frac{m_p}{p}\right) \geq 2^{n/3}(16/1001)^{13-(n-20)/12} \]

\[ = K \exp n(\ln 16 - \ln 13)/12. \]

We have already seen this exceeds 1 for \(n = 20\); it is clearly increasing. Thus it suffices to prove (\(**\)).

Our method will be successive application of Lemma 3 to pairs of factors of \(\prod_p (1 - m_p/p)\). This lemma says that under certain circumstances \((1 - m/p)(1 - m'/p')\) may be replaced by \((1 - (m+u)/p)(1 - (m'-u)/p')\) without increasing the product. Although Lemma 3 only guarantees a positive integer \(u\), the operation may be repeated until \(m + u\) reaches a specified limit (namely, \(r\)) or \(m' - u = 0\). It is easily checked that if \(b' \geq b > 2\), then \(b - b' + r' \leq r\) whether \(r\) and \(r'\) are defined by

1° \( r = b - 1, \quad r' = b' - 1, \)

2° \( r = \lfloor \log_2 b \rfloor, \quad r' = \lfloor \log_2 b' \rfloor, \) or, in case \(b < 13, \)

3° \( r = \lfloor \log_2 b \rfloor, \quad r' = b' - 10. \)

First we use Lemma 3 with \(b = 13, \) \(b' = p_0, \) \(k = m_{13}, \) \(k' = k_0, \) and \(r\) and \(r'\) as in 1°. According to Lemma 3 we can increase \(k\) and decrease \(k'\) (by the same amount) until either \(k + u = r = 12\) or \(k' - u = 0\). Since \(k = m_{13} \leq \lfloor \log_2 13 \rfloor = 3, \) we can guarantee this way that \(k' - u \leq p_0 - 10.\)

In order to avoid a mess we redefine our \(m\)'s so as to denote our new product again by \(\prod_p (1 - m_p/p)\). Now \(m_p \leq p - 10\) for \(p = p_0, \) \(m_{13} \leq 12,\) and \(m_p \leq \lfloor \log_2 p \rfloor\) for all other \(p.\) As before, \(\sum_p m_p = n.\)

Now if \(m_p < \lfloor \log_2 p \rfloor\) for any \(p < 13,\) we apply Lemma 3 to increase \(m_p\) to equal \(\lfloor \log_2 p \rfloor\) by taking away from \(m_p\) for \(p > 13.\) This is justified by taking \(r\) and \(r'\) as in 2° if the larger prime is not \(p_0,\) and 3° if the larger prime is \(p_0.\) Since \(n \geq 20\) all the primes less than 13 can be
"filled up" this way. If we again redefine our $m$'s we now have the product
\[
\prod_p (1 - m_p/p)
\]
\[
\]
where $m_p \leq p - 1$ for $p \geq 13$.

Finally we use Lemma 3 with $r$ and $r'$ as in $1^0$ to stuff any remaining $m_p$'s with $p > 13$ down into 13. If $m_{13}$ gets "filled up" (hits 12) we start a new factor of the form $(1 - \gamma/13)$ by taking $k = 0$ in Lemma 3. This gives
\[
(1 - 1/13)(1 - 2/5)(1 - 2/7)(1 - 3/11)(1 - 12/13)^{(n-8)/12}(1 - \gamma/13),
\]
where $12[(n-8)/12] + \gamma = n - 8$, $\gamma < 12$. Since it is easy to check that $1 - \gamma/13 \geq (1 - 12/13)^{n/12}$, (***) follows.

Of course it remains to show the theorem is true for $n < 20$. This may be checked by more special arguments.

References