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

R. B. CRITTENDEN AND C. L. VANDEN EYNDEN[1]

In 1958 S. Stein [7] defined a system of n congruences $x \equiv a_i \pmod{b_i}$, $1 \leqq i \leqq n$, 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, $1 \leqq x \leqq 2^n$, satisfying none of them. P. Erdös [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.

Erdös 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 $x \equiv 2^{i-1} \pmod{2^i}$, $1 \leqq i \leqq n$, which covers 1, 2, $\cdots$, $2^n - 1$.

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

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

$$x \equiv a_i \pmod{b_i}, \qquad i = 1, 2, \cdots, n.$$

Then there is such an x_0 among $1, 2, 3, \cdots, 2^n$.

LEMMA 1. *Suppose the above theorem is false. Then for some n there exist congruences*

$$x \equiv a_i \pmod{b_i}, \qquad i = 1, 2, \cdots, n$$

such that the following three conditions all hold:

(A) *If $1 \leqq x \leqq 2^n$, 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, $1 \leqq i \leqq n$, such that each x from 1 to 2^n satisfies $x \equiv a_i \pmod{b_i}$ for some i, yet if $T = \{x : x \not\equiv a_i \pmod{b_i}, 1 \leqq i \leqq n\}$, then T is nonempty. Clearly if $x \in T$ and $x \equiv x' \pmod{\mathrm{LCM}(b_1, b_2, \cdots, b_n)}$, then $x' \in T$; thus T contains negative numbers. Let x_0 be the greatest nonpositive element of T. Then the congruences $x \equiv a_i - x_0 \pmod{b_i}$, $i = 1, 2, \cdots, n$, satisfy condition (A).

Let us now suppose the congruences $x \equiv a_i \pmod{b_i}$, $1 \leqq i \leqq n$, 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 $b = p^\alpha q$, where p is prime $q > 1$, $p \nmid q$, and $p^\alpha \nmid a$. Then replacing the congruence $x \equiv a \pmod{b}$ with $x \equiv a \pmod{p^\alpha}$ yields a new set of congruences for which (A) still holds. In fact, if $p \nmid a$ the replacement $x \equiv a \pmod{p}$ works. (The condition $p \nmid a$ 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 $b = p^\alpha$, 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^α 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 $x = 0 \pmod{p}$, 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 $p, 2p, \cdots, [2^n/p]p$, but not 0. Then the $n-k$ congruences $x \equiv a \pmod{b}$ have among their solutions $1, 2, \cdots, [2^n/p]$, 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 $[2^n/p] < 2^{n-k}$. 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 $p \nmid a$,

(2) $x \equiv a \pmod{p^\alpha}$, where $\alpha > 1$ and $p \mid a$,
(3) $x \equiv a \pmod{b}$, where $p \nmid b$.

We may assume each a is positive and less than the corresponding modulus. Since $2^{p-1} \geqq p$ for $p \geqq 2$, (C) implies that there exists a_0, $1 \leqq a_0 < p$, such that $x \equiv a_0 \pmod{p}$ is not one of our congruences. Let $M \equiv \Pi b$, 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 $x \equiv a \pmod{p^\alpha}$ 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^α 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, $1 \leqq x \leqq 2^n$, such that x is in none of the S's. Then if $1 \leqq s \leqq t$, we have*

$$N > 1 + 2^n\left(1 - \sum_{i=1}^{s} k_i/b_i\right) \prod_{i=s+1}^{t} (1 - k_i/b_i) - \left(1 + \sum_{i=1}^{s} k_i\right) \prod_{i=s+1}^{t} (1 + k_1).$$

PROOF. For S any set, let $C(S)$ be the characteristic function of S. First we note that $1 - \sum_{i=1}^{s} C(S_i) \leqq \prod_{i=1}^{s} (1 - C(S_i))$, 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

$$\begin{aligned} C\left(\sim \bigcup_{i=1}^{t} S_i\right) &= C\left(\bigcap_{i=1}^{t} \sim S_i\right) = \prod_{i=1}^{t} C(\sim S_i) = \prod_{i=1}^{t} (1 - C(S_i)) \\ &= \prod_{i=1}^{s} (1 - C(S_i)) \prod_{i=s+1}^{t} (1 - C(S_i)) \\ &\geqq \left(1 - \sum_{i=1}^{s} C(S_i)\right) \prod_{i=s+1}^{t} (1 - C(S_i)) \\ &= 1 - \sum_{i=1}^{t} C(S_i) + \sum_{i,j}{}' C(S_i \cap S_j) - \cdots, \end{aligned}$$

where $\sum'$ indicates that at most one subscript is $\leqq s$.

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

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

Since $[2^n/b_i]k_i \leqq 2^n k_i/b_i < [2^n/b_i]k_i + k_i$, 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 $k_i k_j \cdots k_z$ 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 $|E_{ij\cdots z}| < k_i k_j \cdots k_z$. Then

$$\begin{aligned} N &= \sum_{r=1}^{2^n} C\left(\sim \bigcup_{i=1}^{t} S_i\right)(r) \\ &\geqq \sum_{r=1}^{2^n} \left(1 - \sum_{i=1}^{t} C(S_i) + \sum_{i,j}{}' C(S_i \cap S_j) - \cdots \right)(r) \\ &= 2^n - \sum_{i=1}^{t} 2^n k_i/b_i + \sum_{i,j}{}' 2^n k_i k_j / b_i b_j - \cdots + E \\ &= 2^n \left(1 - \sum_{i=1}^{s} k_i/b_i\right) \prod_{i=s+1}^{t} (1 - k_i/b_i) + E, \end{aligned}$$

where

$$\begin{aligned} |E| &= \left| \sum_{i=1}^{t} E_i - \sum_{i,j}{}' E_{ij} + \cdots \right| \\ &< \sum_{i=1}^{t} k_i + \sum_{i,j}{}' k_i k_j + \cdots = \left(1 + \sum_{i=1}^{s} k_i\right) \prod_{i=s+1}^{t} (1 + k_i) - 1. \end{aligned}$$

The lemma follows.

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

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

PROOF. For $u > 0$ the last inequality is easily seen to be equivalent to $u \geqq b - k - b' + k'$. 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 $k+u=b-b'+k'\leqq b-b'+r'\leqq r$, while $k'-u=b'-b+k\geqq 0$.

LEMMA 4. *If the theorem is false, then it fails for some* $n<20$.

PROOF. Suppose not. Then there exists $n\geqq 20$ 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

$$(*)\qquad 2^n\left(1-\sum_{i=s+1}^{t} k_i/p_i\right)\prod_{i=1}^{s}(1-k_i/p_i)\geqq\left(1+\sum_{i=s+1}^{t} k_i\right)\prod_{i=1}^{s}(1+k_i)$$

for some s, $1\leqq s\leqq t$. We shall take $s=\min([n/3]-1, t-1)$. 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

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

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 $\pi(n-[n/3]+1)\leqq[n/3]$ for small values of $n\geqq 20$; for larger n it follows from known estimates for $\pi(n)$. Thus if $s=[n/3]-1$, we have

$$\sum_{i=s+1}^{t} k_i=n-\sum_{i=1}^{s} k_i\leqq n-[n/3]+1\leqq(\text{the } [n/3]\text{rd prime})<p_{[n/3]}.$$

If we define $k_0=\sum_{i=[n/3]}^{t} k_i$ and $p_0=p_{[n/3]}$, we have

$$(1)\qquad(\text{left side of } (*))\geqq 2^n\prod_{i=0}^{s}(1-k_i/p_i),$$

where $k_0<p_0$, and $k_i\leqq[\log_2 p_i]$ 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

$$\prod_{i=0}^{s}(1-k_i/p_i)=\prod_{p}(1-m_p/p).$$

Since $\sum_0^s k_i\geqq 20$, the conditions $k_0<p_0$ and $k_i\leqq[\log_2 p_i]$ for $i\geqq 1$ imply $p_0\geqq 13$. In particular, $m_2=0$, $m_3\leqq 1$, $m_5\leqq 2$, $m_7\leqq 2$, $m_{11}\leqq 3$, and $m_{13}\leqq 12$. If $p_0=13$, then $n=20$ and

$$\prod_{p}(1-m_p/p)=(1-1/3)(1-2/5)(1-2/7)(1-3/11)(1-12/13).$$

In this case

$$2^n \prod_p (1 - m_p/p) - 4^{n/3} = 2^{2n/3}\left(2^{n/3} \prod_p (1 - m_p/p) - 1\right)$$
$$= 2^{40/3}(2^{10+2/3}/1001 - 1) > 0,$$

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

$$(**)\qquad \prod_p (1 - m_p/p) \geqq (1 - 1/3)(1 - 2/5)(1 - 2/7)(1 - 3/11)\,(1 - 12/13)^{(n-8)/12}.$$

Then

$$2^{n/3} \prod_p (1 - m_p/p) \geqq 2^{n/3}(16/1001)13^{-(n-20)/12}$$
$$= K \exp n(\ln 16 - \ln 13)/12.$$

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 $b'\geqq b>2$, then $b-b'+r'\leqq r$ whether r and r' are defined by

1^0 $r=b-1$, $r'=b'-1$,

2^0 $r=[\log_2 b]$, $r'=[\log_2 b']$, or, in case $b<13$,

3^0 $r=[\log_2 b]$, $r'=b'-10$.

First we use Lemma 3 with $b=13$, $b'=p_0$, $k=m_{13}$, $k'=k_0$, and r and r' as in 1^0. 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 $k=m_{13}\leqq[\log_2 13]=3$, we can guarantee this way that $k'-u\leqq p_0-10$. 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 $m_p\leqq p-10$ for $p=p_0$, $m_{13}\leqq 12$, and $m_p\leqq[\log_2 p]$ for all other p. As before, $\sum_p m_p=n$.

Now if $m_p<[\log_2 p]$ for any $p<13$, we apply Lemma 3 to increase m_p to equal $[\log_2 p]$ by taking away from m_p for $p>13$. This is justified by taking r and r' as in 2^0 if the larger prime is not p_0, and 3^0 if the larger prime is p_0. Since $n\geqq 20$ all the primes less than 13 can be "filled up" this way. If we again redefine our m's we now have the product

$$\prod_p (1 - m_p/p) = (1 - 1/3)(1 - 2/5)(1 - 2/7)(1 - 3/11) \prod_{p \geq 13} (1 - m_p/p),$$

where $m_p \leqq p-1$ for $p \geqq 13$.

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

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

where $12[(n-8)/12]+\gamma = n-8$, $\gamma < 12$. Since it is easy to check that $1-\gamma/13 \geqq (1-12/13)^{\gamma/12}$, (**) follows.

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

References

1. R. B. Crittenden and C. L. Vanden Eynden, *A proof of a conjecture of Erdös*, Bull. Amer. Math. Soc. **75** (1969), 1326–1329.

2. P. Erdös, *Remarks on number theory.* IV: *Extremal problems in number theory.* I, Mat. Lapok. **13** (1962), 228–255. (Hungarian) MR **33** #4020.

3. ———, *Problems* 29 *and* 30, Proc. Conf. Number Theory (Boulder, Colorado, 1963).

4. ———, *Extremal problems in number theory*, Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc., Providence, R.I., 1965, p. 183. MR **30** #4740.

5. John Selfridge, Research announcement, Amer. Math. Soc. Annual Meeting (New Orleans, 1969).

6. ———, *On congruences covering consecutive integers*, Acta Arith. (to appear).

7. S. K. Stein, *Unions of arithmetic sequences*, Math. Ann. **134** (1958), 289–294. MR **20** #17.

Pennsylvania State University,
Portland State University and
Ohio University