A PROOF OF A CONJECTURE OF ERDÖS

BY RICHARD B. CRITTENDEN[1] AND C. L. VANDEN EYNDEN[1]

Communicated by Paul T. Bateman, May 1, 1969

In 1958 S. K. Stein [5] conjectured that if no x satisfied more than one of the congruences

$$x \equiv a_i (\text{mod } b_i), \qquad b_1 < b_2 < \cdots < b_n,$$

then there existed an x, $1 \leqq x \leqq 2^n$, satisfying none of them. P. Erdös proved this with $n2^n$ instead of 2^n [1] and proposed the stronger conjecture that any system of n congruence classes not covering all integers omits a positive integer not exceeding 2^n [1], [2], [3]. Later John Selfridge proved Stein's conjecture [4].

We have proved Erdös's conjecture, and sketch the proof in this note. It is proper to mention that at the meeting of the American Mathematical Society in New Orleans in January 1969, Selfridge, in the course of a ten minute talk on another subject, made an informal preliminary announcement that he had also proved Erdös' conjecture.

Let us suppose the conjecture is false and that n is the smallest number for which it fails.

Claim 1. There exists a set of n congruences such that

(A) each of the integers $1, 2, \cdots, 2^n$ satisfies at least one of the congruences but 0 does not,

(B) all the moduli are prime, and

(C) if k of the congruences have modulus p, then $2^k < p$.

PROOF. By our hypothesis there exist congruences $x \equiv a_i$ (mod b_i), $1 \leqq i \leqq n$, such that if T is the set of integers satisfying none of the congruences, then $x \notin T$, $1 \leqq x \leqq 2^n$, yet $T \neq \emptyset$. T contains negative integers; let x_0 be the greatest nonpositive element of T. Then the congruences $x \equiv a_i - x_0$ (mod b_i) satisfy (A).

Now we assume we have n congruences satisfying (A). Suppose $x \equiv a$ (mod b) is one. Since (A) implies $b \nmid a$, there exists a prime p such that $p^\alpha | b$ but $p^\alpha \nmid a$. Suppose $b = p^\alpha q$. Then we could replace this congruence with $x \equiv a$ (mod p^α) without losing (A). Moreover, if $\alpha > 1$ and $p \nmid a$, our original congruence could be replaced with $x \equiv a$ (mod p), still without losing (A). Thus we may assume all our congruences are of the form $x \equiv a$ (mod p^α) (for various primes p), where $\alpha > 1$ implies $p | a$. This is a start toward (B).

We illustrate our proof of (C) by taking the case $p = 2$. By the last paragraph we can assume our congruences are of three types:

[1] Supported in part by NSF grants GP 6663 and GP 8075.

(1) $x \equiv a \pmod{b}$, b odd,
(2) $x \equiv 1 \pmod{2}$, and
(3) $x \equiv 2a \pmod{2^\alpha}$, $\alpha > 1$.
If the type (2) congruence occurs, then each of the 2^{n-1} even integers between 1 and 2^n must be a solution to at least one of the remaining $n-1$ congruences of types (1) and (3). The same can be said if we replace each type (1) congruence $x \equiv a \pmod{b}$ by $x \equiv a + \epsilon b \pmod{2b}$, where $\epsilon = 0$ if a is even and 1 if a is odd, since no even solutions have been lost.

We now have $n-1$ congruences of the form $x \equiv 2a \pmod{2b}$, having among their solutions $2, 4, 6, \cdots, 2^n$ but not 0. Then each of $1, 2, \cdots, 2^{n-1}$ is a solution to one of the $n-1$ congruences $x \equiv a \pmod{b}$; 0 still is not. This contradicts our assumption that n is the least integer for which the conjecture fails. The proof of (C) for arbitrary prime p is analogous.

Now (B). If p is a fixed prime we know we can assume our congruences are of types
(1) $x \equiv a \pmod{b}$, $p \nmid b$,
(2) $x \equiv a \pmod{p}$, $p \nmid a$, and
(3) $x \equiv a \pmod{p^\alpha}$, $\alpha > 1$, $p \mid a$.
Since $2^{p-1} \geqq p$, (C) tells us there exists x_0 such that $p \nmid x_0$ and x_0 solves no type-(2) congruence. Let M be the product of the moduli of the type-(1) congruences and choose r such that $rM \equiv x_0 \pmod{p}$. It is easily checked that rM satisfies no congruence, even if we change the modulus of each type (3) congruence from p^α to p, since $p \nmid rM$. This loses (A), but (A) can be regained by a shift just as at the beginning of this proof. Q.E.D.

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

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

Proof. Let $N_{ij\cdots s}$ be the number of integers x, $1 \leqq x \leqq 2^n$, in $S_i \cap S_j \cap \cdots \cap S_s$. It is well known that

$$N = 2^n - \sum_{i=1}^{t} N_i + \sum_{i,j} N_{ij} - \sum_{i,j,k} N_{ijk} + \cdots. \tag{1}$$

If $C(S_i)$ is the characteristic function of S_i, it is easily seen that $(1-\sum_{i=s+1}^{t} C(S_i)) \leqq \prod_{i=s+1}^{t} (1-C(S_i))$. From this and

$$\sum_{r=1}^{2n} C(S_i \cap S_j \cap \cdots \cap S_z)(r) = N_{ij\ldots s}$$

we conclude that the right side of (1) is $\geqq$

$$2^n - \sum_{i=1}^{t} N_i + \sum_{i,j}{}' N_{ij} - \sum_{i,j,k}{}' N_{ijk} + \cdots, \tag{2}$$

where $\sum'$ means that only terms with at most one subscript $>s$ are added in.

Since the b's are relatively prime in pairs the Chinese remainder theorem implies that $N_{ij\ldots z}$ counts the solutions of $k_i k_j \cdots k_z$ congruences modulo $b_i b_j \cdots b_z$. Thus $N_{ij\ldots z} = 2^n k_i k_j \cdots k_z / b_i b_j \cdots b_z + E_{ij\ldots z}$, where $|E_{ij\ldots z}| < k_i k_j \ldots k_z$. Substituting this in (2) gives

$$N \geqq 2^n \left(1 - \sum_{i=1}^{t} k_i/b_i + \sum_{i,j}{}' k_i k_j / b_i b_j - \cdots \right) + E,$$

where $|E| < 1 + \sum_{i=1}^{t} k_i + \sum_{i,j}' k_i k_j + \cdots$. The claim follows directly. Q.E.D.

The rest of the proof consists in showing that given a set of congruences as in Claim 1 we can apply Claim 2 so as to prove $N>0$, in contradiction to (A). We sketch the proof for $n \geqq 20$; smaller n can be handled by special arguments. Let there be k_i congruences modulo p_i for $1 \leqq i \leqq t$, where the p's are prime and $p_1 < p_2 < \cdots < p_t$. We take $s = [n/3] - 1$. (If this is more than t everything works with $s = t-1$.) We will show

$$\begin{aligned} &2^n \left(1 - \sum_{i=s+1}^{t} k_i/p_i\right) \prod_{i=1}^{s} (1 - k_i/p_i) \\ &\qquad\qquad \geqq \left(1 + \sum_{i=s+1}^{t} k_i\right) \prod_{i=1}^{s} (1 + k_i). \end{aligned} \tag{3}$$

The right side of (3) has $s+1$ factors with sum $n+s+1$ and so is maximized by $((n+s+1)/(s+1))^{s+1} \leqq 4^{n/3}$. From inspection of a table of primes and known theorems we have $\pi(n-s) \leqq [n/3]$ for $n \geqq 20$; from this we conclude $\sum_{i=s+1}^{t} k_i \leqq n-s < p_{[n/3]}$. Then letting $p_0 = p_{[n/3]}$ and $k_0 = \sum_{i=s+1}^{t} k_i$ we have the left side of (3) is $\geqq 2^n \prod_{i=0}^{s} (1-k_i/p_i)$, where $k_i \leqq [\log_2 p_i]$, $1 \leqq i \leqq s$. By elementary inequalities this product can be seen to exceed

$$2^n\left(1-\frac{1}{3}\right)\left(1-\frac{2}{5}\right)\left(1-\frac{2}{7}\right)\left(1-\frac{3}{11}\right)13^{(8-n)/12}.$$

This is easily seen to be greater than $4^{n/3}$ for $n \geqq 20$.

References

1. P. Erdös, *Extremal problems in number theory*, Mat. Lapok **13** (1962), 228–255.

2. ———, *Problems* 29 *and* 30, Proc. No. Th. Conference, Boulder, Colorado, 1963, p. 96.

3. ———, *Extremal problems in number theory*, Proc. Sympos. Pure Math., vol 8 Amer. Math. Soc., Providence, R. I., 1965, p. 183.

4. J. Selfridge, *On congruences covering consecutive integers*, Acta Arith. (to appear).

5. S. K. Stein, *Unions of arithmetic sequences*, Math. Ann. **134** (1958), 289–294.

The Pennsylvania State University, University Park, Pennsylvania 16802 and
Ohio University, Athens, Ohio 45701