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

$$x \equiv a_i \pmod{b_i}, \qquad b_1 < b_2 < \cdots < b_n,$$

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 $x \equiv a_i \pmod{b_i}$, $1 \leqq i \leqq n$, 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 $T \neq \varnothing$. T contains negative integers; let x_0 be the greatest nonpositive element of T. Then the congruences $x \equiv a_i - x_0 \pmod{b_i}$ satisfy (A).

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